Symantec Mail Security 8160

Implementation Guide

Symantec Mail Security 8160 Implementation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 1.0.2

May 27, 2005

Part Number: 10413014

Copyright notice

Copyright © 1998–2005 Symantec Corporation.

All rights reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, Symantec TurnTide and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. LiveUpdate, LiveUpdate Administration Utility, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection

Contacting Technical Support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

http://www.symantec.com/techsupp/enterprise/

When contacting the technical support group, please have the following:

- Product release level
- Hardware information
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
- Error messages/log files
- Troubleshooting performed prior to contacting Symantec
- Recent software configuration changes and/or network changes

Contents

Chapter 1 Introducing Symantec Mail Security 8160

About Symantec Mail Security 8160 9
Specifications 9
Supported USB CD ROM drives 10
Front panel indicators 10
The Control Center 11
Accessing the Control Center 11
Control Center permissions 12

Chapter 2 Preparing to set up Symantec Mail Security 8160

Deployment Planning 13
Installing the appliance 14
Controlling traffic - Passthrough 14
Controlling traffic – Active Mode 15
Operating modes and configuration considerations 15
Virtual Bridge Mode 16
Router Mode 17
High availability and clustering 18
Bridged active-passive 19
Routed active-passive 19
MX active-active 19
Data Synchronization 19
Advanced Failover 19
Placement considerations 20
Installing in multiple locations 20
Firewall considerations 20
Port access requirements 21
Addressing for high availability implementations 21
Security considerations 22

Chapter 3 Configuring Symantec Mail Security 8160

Installation and deployment time 23
Before you begin 24
About configuring Symantec Mail Security 8160 25
Identifying the network adaptors 25

Initializing Symantec Mail Security 8160 25
Registering your appliance 26
Setting up your appliance 28
Before you configure 28
Configuring Symantec Mail Security 8160 28
Configuring multiple appliances 35
About configuration 36
Exporting a configuration 36
Importing an existing configuration 36
Reverting settings 37
Synchronizing data between appliances 37
About advanced failover 38
Required IP addresses 39
Virtual IP responsibility level 39
Virtual Router IDs 39
Configuring advanced failover 40
Example advanced failover configuration 41

Chapter 4 Working with Traffic Control

About Traffic Control 43
Changing Traffic Control levels 44
Changing Traffic Control to Passthrough mode 44
Changing the level of active control 44
Tuning Traffic Control manually 45

Chapter 5 Working with graphs and reports

Viewing current path statistics 50
Viewing available graphs 50
Connection load graph 51
Bandwidth utilization graph 51
Message load graph 51
Path quality statistics graph 51
CPU utilization graph 51
Modifying graph display and saving graph data 52
Changing the graph time frame 52
Exporting the graph data 52
Viewing current network statistics 53
External network 53
Protected network 53
Arp Table 53
Viewing System Status 53
Viewing the Event Log 54

Viewing overall path statistics 54
Viewing email traffic estimates 55
Viewing overall performance 55
Viewing and creating reports 56
Data sources for custom reports 57

Chapter 6 Working with network path information

About network path information 59
Searching network path information 60
Modifying network path information 61
Changing a path's assumed spam rate 62
Viewing manually altered paths 63
Making bulk changes to network paths 63
Uploading whitelisted or blacklisted paths in bulk 64
Maintaining the paths database 64
Backing up path data 65
Restoring path data 65

Chapter 7 Administering Symantec Mail Security 8160

Starting, stopping, or powering down 68
Stopping services (switching to Inactive mode) 68
Starting services (switching to Active mode) 68
Powering down and rebooting the appliance 69
Viewing the Changelog 69
Administering user accounts 69
Changing a user password 70
Adding a new user account 70
Deleting a user account 71
Modifying an existing user account 72
Troubleshooting 72
Software updates from Symantec 72
Setting up alerts 73
Managing Licenses 74

Appendix A Example Deployment Scenarios

High availability virtual bridge implementation 76
High availability router implementation 77
Mail server gateway router implementation 78
Policy routed router implementation 79

Appendix B Command Line Interface Reference

bootstrap 81
clear 82
grep 82
help 82
ifconfig 82
iostat 82
netstat 82
nslookup 83
passwd 83
ping 83
reboot 83
rebuildrpmdb 83
restore-config 83
route 84
service 84
showarp 84
shutdown 84
system-stats 84
tail 85
traceroute 85
update <option> 86
version 86
watch 86

Appendix C SNMP MIB Reference

Index

Chapter 1

Introducing Symantec Mail Security 8160

This chapter includes the following topics:

- About Symantec Mail Security 8160

About Symantec Mail Security 8160

The unique system design of Symantec Mail Security 8160 helps to reduce the amount of unwanted email entering enterprise networks by analyzing your network's email flow and identifying the behavior of various network paths over time.

Symantec Mail Security 8160 identifies spammers by pinpointing the true source of each email. The 8160 then limits the bandwidth and resources that spamming sources can use, significantly decreasing the flow of spam. It helps to prevent spam at its source, keeping it off your network and eliminating false positives.

Using Transmission Control Protocol (TCP) traffic shaping at the TCP protocol level, the 8160 manages the quality of service that each email sender is given based on how likely it is that they are sending spam. Legitimate senders receive excellent quality of service and their mail flows quickly, while spammers are given very poor quality of service and their mail is slowed dramatically. Spammers have no way to force mail into your protected network, so their spam simply backs up on their own servers.

Specifications

Each compact, rack-mounted, 1UIntel-based server appliance is based on proven hardware custom-manufactured by Dell, with all necessary operating system

and product software pre-installed. The appliance and included software ship pre-hardened against common vulnerabilities and attacks.

Symantec Mail Security 8160 is powered by two 3.2 GHz Intel Xeon processors, 2GB of RAM, two 80GB hard drives in a RAID1 configuration, and hot-swappable power supplies and fans.

Supported USB CD ROM drives

The following USB CD drives are supported (but not included):

- Dynex DX-ECDRW100
- IOMEGA CD-RW CDRW55292EXT
- TEAC CD-210PU
- Memorex Ultra Speed CD Recorder CD-RW - Hi-Speed USB

Front panel indicators

The two system identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pushed, the blue system status indicators on the front and back of the system blink. (To stop the indicator from blinking, press one of the identification buttons a second time.)

LED Indicator	Description
Blue/amber system status indicator	The blue system status indicator lights up during normal system operation. The amber system status indicator flashes when the system needs attention due to a system problem.
NIC1 and NIC2 link indicators	The indicators for the two integrated network adapters light if the network adapters are connected to the network. NIC1 corresponds to interface Eth0. NIC2 corresponds to interface Eth1.

LED Indicator	Description
Power indicator	The green indicator in the center of the power button flashes if AC power is available to the system, but the system is not powered on. The green indicator is on when the system is powered on. If the system is not connected to AC power, the green indicator is off.

The Control Center

Symantec Mail Security 8160 provides a secure, powerful Web-based administrative interface known as the Control Center. The Control Center lets you monitor, configure and administer your Symantec Mail Security 8160 installation.

Using the features of the Control Center you can:

- Monitor and manage the performance of your Symantec Mail Security 8160 installation
- Add, delete, and manage users of the Control Center
- Turn off and power down the Symantec Mail Security 8160

Accessing the Control Center

Once you have completed setting up Symantec Mail Security 8160 as described in the next chapters, you can use your Web browser to access the Control Center.

The Control Center supports all HTML 4.0 compliant Web browsers, including:

- Microsoft Internet Explorer (version 6 or later)
- Netscape Navigator version (7 or later)
- Mozilla
- Firefox 1.0

Note: Symantec 8160 uses a self-signed certificate to provide SSL security for the web based Control Center. You must accept this certificate to gain access to the Control Center.

Control Center permissions

The Control Center is a password-protected application that also lets administrators control the level of user access by assigning each user to one or more groups, which determines the functions that each user can perform.

Group name	Access
User	Read-only access to monitoring data (Users can change their own password). All users are members of this group.
Data Admin	Configure and administer network paths influenced by Symantec Mail Security 8160.
User Admin	Add, delete, and manage users of the Control Center.
System Admin	Administer the appliance, including system control and software updates.
Master Admin	Perform all tasks available to all groups. A Master Admin account can not be seen or edited by any user that is not a Master Admin.

Your user name can be assigned to one or more of the above groups, which determines the roles that are accessible to you in the Control Center.

Chapter 2

Preparing to set up Symantec Mail Security 8160

This chapter includes the following topics:

- Deployment Planning
- Operating modes and configuration considerations
- Placement considerations

Deployment Planning

The Deployment Overview provides a high level walkthrough of the process of integrating the Symantec Mail Security 8160 into a network's mail stream at a high level.

The first thing to determine when planning Symantec Mail Security 8160 deployment is where email enters your network. Multiple physical sites may require multiple appliances, depending on where the mail systems that will be protected are located.

Next, consider the location within the network of the mail servers themselves. Symantec Mail Security 8160 is deployed on the network "upstream" of the mail servers to be protected. All inbound mail and the return traffic must flow through the appliance.

In order to accommodate a wide variety of network architectures, Symantec Mail Security 8160 can be installed as a Virtual Bridge (using proxy ARP), or a Router.

The Virtual Bridge deployment is the easiest to configure, as it generally does not require re-configuration of any upstream routers or the protected mail servers. It is best suited to networks where all protected mail servers reside on the same layer two network. As a Virtual Bridge, Symantec Mail Security 8160 is normally placed directly in front of the mail servers it is protecting, and all network traffic to and from those servers goes through the appliance. Details on deploying as a Virtual Bridge, including restrictions, are in "Virtual Bridge Mode" on page 16.

The Router deployment is better suited to networks where the protected mail servers are on different layer two networks, or the existing network architecture is too complex for the Virtual Bridge deployment. Details on deploying a simple Router configuration are in "Router Mode" on page 17.

Additional deployment scenarios, including using policy routing to direct only SMTP traffic through the 8160, can be found in "Example Deployment Scenarios" on page 75.

To support high availability requirements, multiple Symantec Mail Security 8160 appliances can be deployed in a cluster. In a cluster, data is synchronized between appliances to insure the secondary (or backup) appliance is always up to date. A detailed discussion of high availability options for Symantec Mail Security 8160 is in "High availability and clustering" on page 18.

Installing the appliance

Installation of Symantec Mail Security 8160 is accomplished in two stages. At initial boot, you log on at the command line and are prompted for the basic information needed to get the appliance on the network. After the appliance is 'bootstrapped' onto the network, you use a web browser to perform the remaining configuration using the browser-based Control Center.

Controlling traffic - Passthrough

When Symantec Mail Security 8160 is first installed, it comes up in Passthrough mode, where no traffic control is applied. In Passthrough mode, the appliance examines mail from source Paths (IP addresses), rating the mail as to the probability it is spam, and recording the results for each Path in the internal database.

Symantec Mail Security 8160 should be left in Passthrough for a minimum of 24 hours, but up to a week is recommended. This gives the appliance sufficient time to correctly learn about the Paths that regularly send mail to your network. The longer the time the appliance is in Passthrough, the more effective it will be when moved to 'Active' mode. Details on Traffic control can be found in "Working with Traffic Control" on page 43

Controlling traffic – Active Mode

The final step in deploying Symantec Mail Security 8160 is moving the appliance from Passthrough to Active mode. In addition to examining mail and storing ratings just as Passthrough does, Active mode applies traffic control to all messages sent through it. Instructions for switching the appliance to Active mode are found in "Working with Traffic Control" on page 43.

There are five stages of Traffic Control shipped with Symantec Mail Security8160. Each stage more aggressively controls mail from spamming Paths. As with Passthrough mode, switching from stage to stage should be done in measured steps to allow Symantec Mail Security 8160 to continue to learn about your mail

The following guidelines are recommended for the amount of time to stay in each Traffic control "stage"

Table 2-1 Traffic Control Guidelines

Stage	Minimal time	For a small mailstream	For a large mailstream
Passthrough	24hrs	5-7 days	3-5 days
Stage 1 - 5	24 hrs	3-5 days	1-3 days

Operating modes and configuration considerations

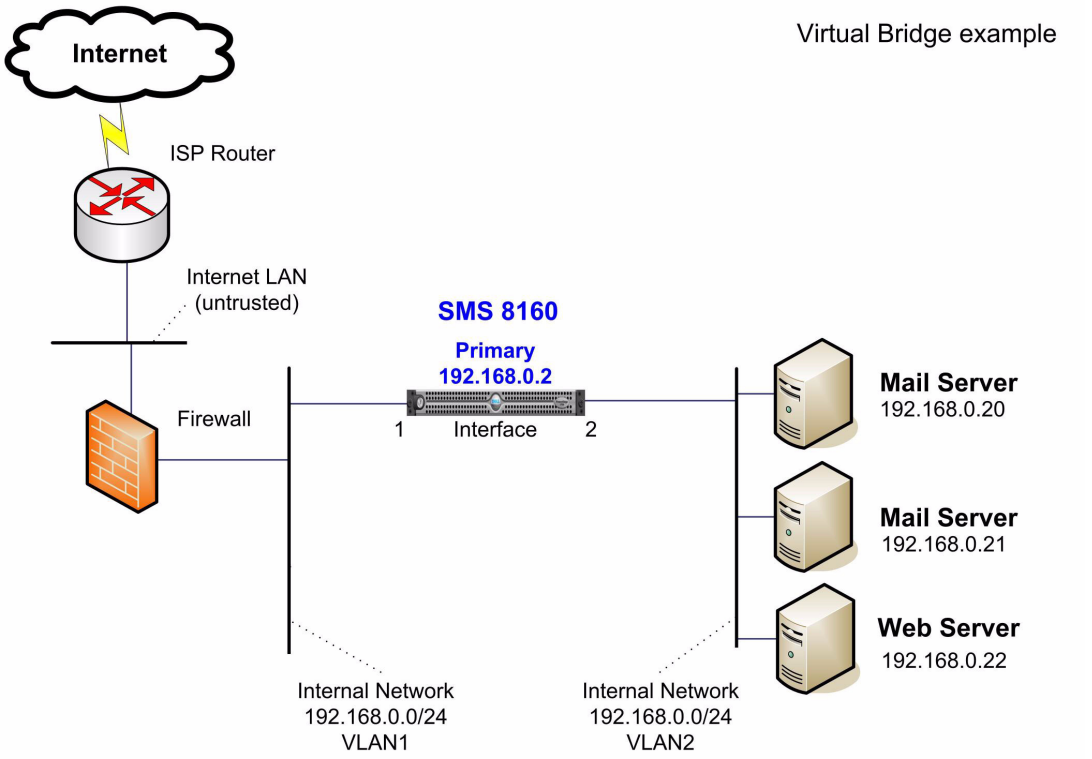
You can install Symantec Mail Security 8160 in one of two operating modes, depending on the characteristics of the network into which it is inserted. In addition to the diagrams in the following sections, refer to "Example Deployment Scenarios" on page 75 for other possible deployment options.

Virtual Bridge Mode

In Virtual Bridge mode, 8160 appliances bridge traffic between parts of the same subnetwork. In this mode, you do not need to make any routing changes to the configuration of any devices upstream or downstream of the 8160. Service interruptions for installation of bridge mode deployments are typically less than 10 minutes. This mode is recommended for simpler network architectures, where the flexibility of routed mode is not required. The internal and external interfaces must be on separate Layer 2 networks. In many networks, a VLAN is used to segment a switched network on a logical, rather than physical basis. You can insert a Symantec Mail Security 8160 into a network by linking VLANs.

Note: You cannot use the 8160 in Virtual Bridge mode in front of a router in a network using active routing protocols (such as OSPF).

Figure 2-1 Example of a Virtual Bridge implementation

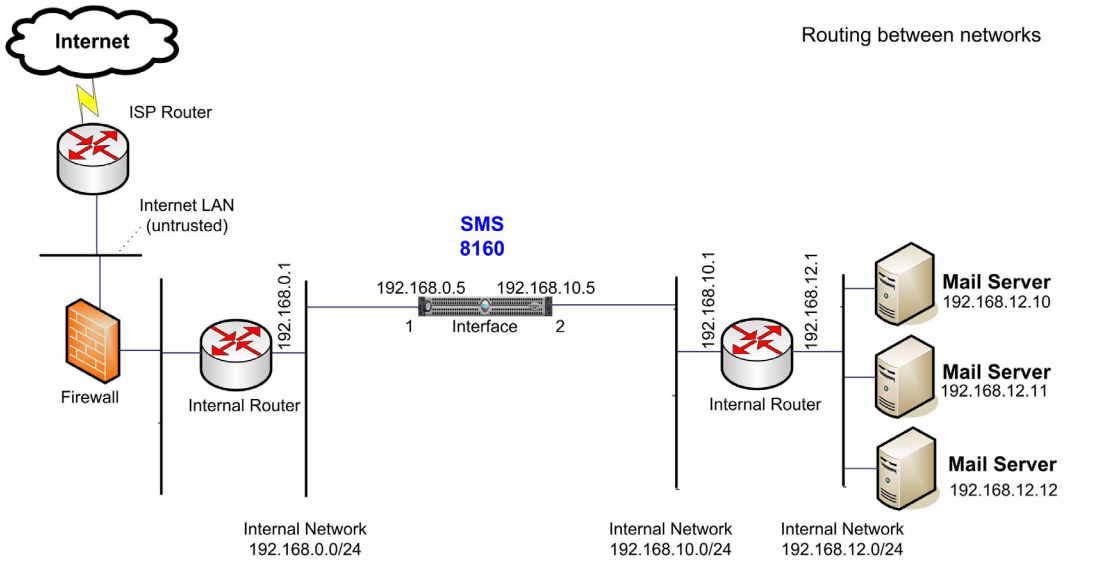


Router Mode

In Router mode, Symantec Mail Security 8160 appliances route traffic between two or more separate routed subnetworks. In this mode, you will most likely have to change gateways and routes both upstream and downstream of the appliance(s). This mode is recommended when the complexity of the protected network precludes bridging.

In Router mode, the return traffic must also be routed through the appliance. If your site passes a very high level of traffic, you may wish to implement a policy routed setup (such as the one described in "Policy routed router implementation" on page 79).

Figure 2-2 Example of a Router implementation



High availability and clustering

Symantec Mail Security 8160 appliances are reliable, robust devices capable of handling large volumes of traffic. However, in any environment where high availability is a key requirement, fault tolerance and redundancy is generally designed into the network architecture. It is generally recommended that you match the existing level of high availability in your protected email infrastructure when you deploy Symantec Mail Security 8160.

Since the 8160 is a high throughput device, clustering for capacity purposes is needed only in the very largest of environments. More frequently, clustering is deployed to provide high availability. Active-passive clustering configurations serve this purpose.

The high availability feature uses the VRRP protocol to communicate availability between appliances.

To select a **router** configuration and implement high availability (using two 8160 appliances):

- You must allocate the following IP Addresses:
  - One IP address for each physical interface (four total)
  - One virtual IP address on the external network.
  - The upstream devices (such as routers) direct mail to this IP address.
  - One virtual IP address on the internal network.
    The downstream devices (such as mail servers) direct return traffic to this IP address.
- You must also designate a virtual router ID (VRID) for the pair of appliances that is unique on the external subnet, including any other VRRP instances.

An example of a highly available router configuration is described in "High availability router implementation" on page 77.

To select a **virtual bridge** configuration and implement high availability, you must designate a virtual router ID (VRID) that is unique on the external subnetwork (including any other VRRP instances) for the pair of appliances.

An example of a highly available virtual bridge configuration is described in "High availability virtual bridge implementation" on page 76.

Bridged active-passive

Bridged configurations implement active-passive clustering by virtualizing the bridging responsibility across the two cluster members. In the event of a component failure, bridging responsibility is immediately transferred to another cluster member, and all appropriate ARP entries on network peers are updated. The transfer of bridging responsibility is transparent to existing sessions.

Routed active-passive

Routed configurations implement active-passive clustering by virtualizing gateway addresses on all networks across the two cluster members. In the event of a component failure, the gateway addresses are immediately transferred to another cluster member, and all appropriate ARP entries on network peers are updated. The transfer of gateway addresses is transparent to existing sessions.

MX active-active

Most large environments have primary and secondary MXs in different physical locations. MX active-active clustering places an 8160 in front of each MX, protecting the network from spam traffic while using the existing multiple MX implementation high availability. This is accomplished using the Data Synchronization feature described in "Synchronizing data between appliances" on page 37.

Unless high availability strategies within each physical location require additional clustering, MX active-active with a distributed cluster made up of one cluster member per physical location can be used.

Data Synchronization

The 8160 can also synchronize network path information between appliances. This is used to keep appliances in a local high availability installation up to date as well as distributed clusters such as an MX-MX active deployment.

Advanced Failover

The Advanced Failover feature of Symantec Mail Security 8160 allows the appliance to participate as a primary or backup device in a cluster of up to four appliances. It is intended to offer a high level of redundancy in dual-homed, policy routed configurations For more information about advanced failover, refer to "About advanced failover" on page 38.

Placement considerations

As a device, the essential role of Symantec Mail Security 8160 is to act as a router or a virtual bridge in a network. As such, it should be placed into the network at a point upstream of the email infrastructure. The portion of the network downstream of the 8160 is known as the “protected network”.

You can place Symantec Mail Security 8160 inside or outside firewalls and in front of all types of network traffic; all non-email traffic passing through the appliance is forwarded without any inspection or control.

Keep the following in mind:

- Access to the original TCP session between the Internet and the protected mail servers (including non-NAT-ed source addresses) is required in order to control resource allocation. Destination NAT, however, is acceptable.
- Do not deploy a load balancer in front of multiple instances of Symantec Mail Security 8160. Load balancers for your mail servers behind the 8160 are acceptable.
- You cannot use the 8160 in Virtual Bridge mode in front of a router in a network using active routing protocols (such as OSPF).
- In Router mode you must ensure the return traffic is also routed through the appliance.

Installing in multiple locations

If your email network has several entry points (either physical or logical), you may wish to install an 8160 to protect each individual physical or logical entry point. Commonly, most email infrastructure deployments include multiple email servers. A single Symantec Mail Security 8160 can protect a large cluster of email servers – some installations protect hundreds of email servers. In situations where high availability and failover is required, you can deploy Symantec Mail Security 8160 appliances in clusters. The important points to remember are to place the 8160 upstream of the email infrastructure (often before the first gateway MTA server), and that in most cases, multiple entry points into the networks email servers are protected by multiple appliances. You may wish to use the Advancd failover features described in “Advanced Failover” on page 19.

Firewall considerations

Generally, you should place Symantec Mail Security 8160 behind the firewall. However, you cannot place the 8160 behind firewalls that implement full store-and-forward SMTP proxies. You should also not place the appliance behind full

TCP proxies. Access to the original TCP session between the Internet and the protected mail servers (including non-NAT-ed source addresses) is required in order to control TCP resource allocation.

You can use a full-TCP proxy firewall, but you must disable the proxy for the SMTP port; consult your firewall documentation for details

Port access requirements

All Symantec Mail Security 8160 appliances need access to the Symantec central servers for software and security updates.

In addition:

- Local TCP/53 and/or UDP/53 access to local DNS servers is required.
- TCP/443 access to the 8160 is required from networks that are to be allowed access to the Control Center (the Web-based administration interface) and also to the Symantec licensing server.
- TCP/443 access must be allowed to the Symantec Licensing server.
- TCP/123 access for NTP servers.
- If multiple 8160 appliances are deployed in a cluster, bidirectional access to TCP/22 is required for all members of the cluster to support data synchronization within the cluster.

Addressing for high availability implementations

For a **Virtual Bridge** configuration, you must allocate the following IP addresses:

- One IP address for each physical appliance (two total)
- The upstream devices (such as routers) direct mail to the IP address of the mail server(s) on the protected network.
- The downstream devices (such as mail servers) direct return traffic to the same gateway device IP address they did before the 8160 was put in place.

For a **router** configuration, you must allocate the following IP addresses:

- One IP address for each physical interface (four total)
- One virtual IP address on the external network.
  The upstream devices (such as routers) direct mail to this IP address.
- One virtual IP address on the internal network. The downstream devices (such as mail servers) direct return traffic to this IP address.

- You must also designate a virtual router ID (VRID) that is unique on the external subnetwork (including any other VRRP instances) for the pair of appliances.
  An example of a high available router configuration is described in "High availability virtual bridge implementation" on page 76.

Note: It may be helpful for you to make a list of every single physical and virtual address on the layer 3 network that will be located behind Symantec Mail Security 8160 as you will have to designate each of them as a protected server. Do not include IPs that are on the external (not-protected) network, or portions of your network may become unreachable.

Security considerations

Symantec Mail Security 8160 was designed from the ground up to meet the stringent security requirements of the networks in which it is deployed. The appliance incorporates a stateful inspection firewall primarily to protect itself from outside attack. Access to the appliance is encrypted at all times, and is authenticated using multiple factors.

Chapter 3

Configuring Symantec Mail Security 8160

This chapter includes the following topics:

- Installation and deployment time
- Before you begin
- About configuring Symantec Mail Security 8160
- Initializing Symantec Mail Security 8160
- Setting up your appliance

Installation and deployment time

Installation and deployment of Symantec Mail Security 8160 ranges in complexity from that of adding a transparent network component to the existing environment (Virtual Bridge Mode) to that of adding a router and additional subnetworks to the existing environment (Router Mode). Most deployments use the Virtual Bridge Mode, and are extremely straightforward. Virtual Bridge Mode deployments are typically completed with less than 10 minutes of service interruption to the email environment.

Before you begin

To install the 8160, you will need the following information:

For Virtual Bridge Mode

- Valid License file from Symantec
- Hostname, including domain (FQDN)
- IP address and netmask for the appliance (in virtual bridge mode, only 1 IP per appliance is needed)
- If implementing a high availability cluster at the same location
  - IP address & netmask for the second appliance
  - VRID for both appliances
- Domain Name servers (DNS)
- NTP Servers (optional)
- List of Protected servers

For Routed mode

- Valid License file from Symantec
- Hostname, including domain (FQDN)
- IP address & netmask for the External interface
- IP address & netmask for the Internal Interface
- If implementing a high availability cluster as the same location:
  - IP address & Netmask for the External interface for the second appliance
  - IP address & netmask for the Internal Interface for the second appliance
  - Virtual IP and netmask for the External interface
    This is the IP address to which inbound mail is sent
  - Virtual IP and netmask for the Internal interface
    This is the IP address to which return traffic is sent
  - VRID for the appliances
- Domain Name servers (DNS)
- NTP Servers (optional)
- List of Protected servers

About configuring Symantec Mail Security 8160

To configure a new 8160, you must do the following

1. Plug in, power up, and initialize the appliance.
2. Register the appliance.
3. Run the Setup Wizard to configure the network and other appliance settings.

These tasks are described in detail in the following sections.

Identifying the network adaptors

When looking at the rear of the appliance, the network connectors are located towards the right hand side of the back plate. Interface 1 is the right hand connector and interface 2 is the left hand connector.

Warning: YOU **MUST** FULLY CONFIGURE THE SYSTEM BEFORE IT WILL BRIDGE TRAFFIC. CONNECT THE EXTERNAL INTERFACE (LABELED INTERFACE 1) TO THE NETWORK BUT **DO NOT** PLUG IN THE INTERNAL INTERFACE (LABELED INTERFACE 2) UNTIL YOU HAVE SUCCESSFULLY COMPLETED CONFIGURATION.

Initializing Symantec Mail Security 8160

When you first power up your appliance, you will perform a one-time initialization sequence to get it up and running.

To initialize your new appliance

1. Unpack the appliance and either rackmount it or place it on a level surface.
2. Plug in AC power.
3. Connect a keyboard and VGA monitor to the appliance.
4. Connect an ethernet cable to the external (eth0, interface 1) interface jack on the back panel.
   When looking at the rear of the appliance, the network connectors are located towards the right hand side of the back plate. Interface 1 is the right hand connector and interface 2 is the left hand connector.
5. Switch on the power.
   The appliance will boot up.

6 Log in on the console and change your password.
The starting login information is:
- username: **admin**
- password: **symantec**

7 Type your new password twice when prompted.
You are next asked for the host name.

8 Type a fully qualified name for this host.
For example:
`hosta.companyb.com`
Next, you will be asked to supply the IP address for the Ethernet port labelled **1** on the back of the appliance. When looking at the back of the appliance, it is the connector on the right hand side.

9 Enter the IP address for this appliance. For example:
`192.168.0.1`
You are asked for network addressing information.

10 Enter the additional network information for this appliance when prompted (netmask, broadcast address, network address, default gateway, and nameserver).
The interface will default to the correct values for the broadcast and network addresses.

11 Set the Timezone, Date and Time for the appliance.

12 If the summary information is correct, type **Y**, if not type **N** and make changes.
The appliance will reboot. Once it has finished, continue with the next procedure, "Registering your appliance" on page 26.

Registering your appliance

After you complete the initialization process, you must log into the Control Center using the password you set during initialization in order to register the appliance. You can access the appliance from any computer that can connect to the appliance using a Web browser.

To complete registration, you will need the license file (.slf file) provided to you by Symantec. Place this file on the computer from which you are accessing the Control Center.

To register your appliance

1. From a computer that can access the new appliance, log into the appliance using a browser.
   The default login address is:
   https://<IP-address>
   where **<IP-address>** is the IP address you designated for your appliance during initialization. The default port, which you do not need to enter, is 443.
   Accept the self-signed SSL certificate.
   The Control Center log in page is displayed.
2. Log in as user **admin**, using the password you set during initialization.
   The Appliance Registration page is displayed, showing the license status of each feature.
3. On the Licensing page, select the **From a file on my computer** radio button, then click **Browse** to find your .slf file.
   If you have other Symantec license files, be sure you select the correct one.
4. Select your .slf file and click **Open** to return to the Licensing page.
5. Click **Install**.
   - If registration was successful, the Appliance Registration page is redisplayed.
   - If there was an error, you will see error text at the top of the page; visit Symantec's support Web site for assistance. Check to make sure the appliance you are registering has net connectivity. Log into the command line interface and ping an outside network site by its domain name. If you do not have connectivity from the appliance, you may have mis-configured the IP or gateway address during initialization. If this is the case, you may wish to repeat the initialization procedure. To do this, log in to the console as user **admin**, and from the command line, type:
     bootstrap --reconfigure
     and proceed through the initialization process described in "Initializing Symantec Mail Security 8160" on page 25.
6. When your .slf file is successfully registered, click **Next** to proceed to the Software Update Page.
7. If your software must be updated, click **Update** to update your software. After the update, you will be logged out and the appliance will reboot. The next time you log in, the Setup Wizard will be displayed.
8. Proceed to the next section, "Setting up your appliance" on page 28.

Setting up your appliance

In order for the 8160 to begin traffic-shaping, you must provide it with information about where it is in your network infrastructure, and about how to direct network traffic.

Warning: You should not plug the internal (interface labeled 2) interface jack into the network until you have successfully completed setting up the appliance.

Warning: Until you have activated the configuration, the 8160 will not bridge or route traffic to the protected network. Placing your mail servers on the protected network before you are ready to activate a configuration will cause an interruption in service.

Before you configure

The first time you log into Control Center after initializing and registering the appliance, the Setup Wizard runs, allowing you to configure your appliance. Navigate back and forth within the pages of the wizard using the Next and Back buttons at the bottom of each page.

To reach the Setup Wizard again in the future, log into Control Center, click Settings at the top of the page, and choose Edit Settings from the left hand menu. To confirm and activate new settings, you must click Activate Settings, which will reboot the appliance and apply the new settings.

When you edit the settings on an appliance, but have not yet clicked Activate Settings, the Settings tab will display an asterisk (*) to let you know that you have not yet activated the changes you made. You can cancel on any page, or clear your changes by reverting to previous settings. For more information about reverting settings, refer to "Reverting settings" on page 37.

Note: With the exception of the Set Time Now function, no configurations changes will take effect until you complete the wizard and click Activate Settings on the last page.

Configuring Symantec Mail Security 8160

The following procedures describe how to set up two 8160 appliances in a high availability configuration as either a virtual bridge or as a router. If you are installing a single appliance, you can skip the high availability steps.

If you have multiple Symantec Mail Security 8160 appliances to set up, you may wish to refer to "Configuring multiple appliances" on page 35 for options.

To configure the 8160, log into Control Center, click Settings at the top of the page, and choose Edit Settings from the left hand menu. If this is the first time you are configuring this appliance, the Setup Wizard runs automatically.

- To begin, click **Next**.

Setting up DNS

The first panel of the Setup Wizard is the DNS Setup panel. The values you entered during the initialization process are entered by default.

1. Specify up to three domain name system (DNS) servers to use.
   You must use IP addresses to specify the DNS Servers, not hostnames. Symantec Mail Security 8160 will use these DNS servers to perform DNS lookups.
2. If you wish, change the hostname of your appliance.
3. Click **Next**.

Setting up interfaces

The Interface Setup panel is displayed.

On this panel, you can specify how the network interfaces are configured.

Note: Make sure you set the speed correctly for your network. The most common cause of intermittent network problems is misconfigured network speed and duplex problems, as many common networking products do not auto-negotiate properly.

---

4. Select **Auto** to tell the appliance to auto-negotiate with the switch for this interface, or **Lock** if you would like to specify a rate.
   If you choose **Lock** for one or both interfaces, you must set the interface to duplex speed.
5. Select full or half duplex, and a speed of 10/100/1000(gigabit) for the interface(s).
6. Click **Next**.

Specifying time settings

The Time Settings panel is displayed.

7. On the Time Settings panel, specify your system-wide time settings.

You can change the timezone from what was specified during initialization, reset the date and time on the appliance, and configure the system to use NTP.

Two NTP servers are configured by default. You can use these, replace them with ones of your choice, or disable NTP by deleting all of the entries.

Note: As mentioned at the beginning of the Setup Wizard procedure, if you click the **Set time now** button, the system timezone and time are set on your appliance immediately; you do not have to proceed to the Settings Activation panel and confirm before this setting takes effect.

---

8 Click **Next**.

Specifying management access

The Management Access panel is displayed.

On this panel, you can specify CIDR blocks from which access is allowed to Control Center and the SNMP server. This means that only IPs in the specified CIDR block(s) will be able to connect to Control Center or receive SNMP data. You can specify allowed blocks one at a time, or upload a file containing one CIDR block per line.

Note: If you do not specify one or more allowed CIDR blocks, all IPs are allowed to access Control Center and retrieve SNMP data.

---

9 To add allowed CIDR blocks:

- Enter a CIDR block into the **CIDR block:** field and click **Add Access**, or
- Enter the path to a file containing the list of allowed CIDR blocks into the **Access List Upload** field or browse for the file, and click **Upload Access List**.

  The file containing the list must be browsable from the machine you are currently using to access the Control Center.

The allowed blocks are displayed in the Management Access list.

10 To remove a block's access, select it from the Management Access list and click **Remove Access**.

11 Click **Next**.

Choosing virtual bridge vs. routed configuration

The Bridged vs. Routed panel is displayed.

Depending on the requirements of your network infrastructure, you can specify that Symantec Mail Security 8160 act as a virtual bridge or as a router.

Note: You cannot use the 8160 in Bridged mode in front of a router in a network using active routing protocols (such as OSPF).

12 Choose a configuration:

- If you want to configure the 8160 as a router, choose **Routed Configuration.**
- If you want to configure the 8160 as a virtual bridge, choose **Bridged Configuration**.

If you wish to configure your Symantec Mail Security 8160 installation for high availability, you must have two appliances in the same location. You will designate one as the primary appliance, and one as the secondary appliance. The primary appliance will synchronize data to the secondary appliance.

13 If you are configuring a single 8160 appliance and will not add a second for high availability in the same location, skip to step 17.

Note: If you select a router configuration, you must allocate a third IP address to use as a virtual IP for both appliances (in addition to the IP each appliance has on the real network.

To configure for high availability

14 From the Bridged vs. Routed panel, specify whether this is the primary or secondary appliance.

This configuration procedure is the same for both the primary and secondary appliance, with the exception of the Key Management panel, described in step 29.

If you chose a Routed Configuration, are configuring for high availability, and have multiple pairs of 8160 appliances, you may want to set up advanced failover. Advanced failover supports transparent failover from failure of up to all but a single member of the group of clusters. For more information about advanced failover, refer to "About advanced failover" on page 38.

15 Click **Next**.

Setting up virtual bridge or routed configuration

Depending on which you chose on the previous panel, the Bridged or the Routed configuration panel is displayed.

16 Enter configuration information:

- If this is a Virtual Bridge configuration, enter the IP address, netmask, virtual router ID, and gateway for Symantec Mail Security 8160.
- If this is a Routed configuration, enter the IP address, netmask, virtual IP address, and virtual router ID for each interface, and specify the default gateway and the interface to which it is attached.
- Enter the unique Virtual Id identifying this appliance pair.

17 If you want to specify additional network routes, check the **Advanced Routes** box, click **Next**, and proceed to the next section "Setting up network routes" on page 32. Otherwise, leave the box unchecked, click **Next**, and skip to "Setting up protected servers" on page 32.

Setting up network routes

The Advanced Routes panel is displayed.

Routes you specify here are added to the routing table for special network situations.

18 Click **Next**.

Setting up protected servers

The Protected Servers panel is displayed.

19 Add the IP addresses and gateway for any systems that are on the LAN or VLAN behind Symantec Mail Security 8160.

- For a virtual bridge configuration, you must add every host behind the 8160. This includes non-mail traffic. Hosts on the protected network that are not in the Protected servers list will not be accessible from the external network.
- For a routed configuration, you must also add the next-hop gateway to each protected host.

If there is an intermediary router between the 8160 and the mail servers, the next-hop gateway is the IP address of the router. If there is no intermediary router between the 8160 and the mail servers, then the next-hop gateway should be set to 0.0.0.0. Refer to the High availability router implementation and Mail server gateway router implementation examples in "Example Deployment Scenarios" on page 75.

Bulk uploading protected hosts

If you have a large list of hosts you are protecting, you can upload them through the browser.

- For a virtual bridge configuration, the file format is a plain text file consisting of one IP address per line

For example:

```
192.168.3.3
192.168.3.4
```

- For a routed configuration, the file format is a plain text file, each line consisting of the protected server IP address, a comma, and the next hop gateway address.

  For example:

  ```
  192.168.3.3,192.168.3.254
  192.168.3.4,192.168.3.254
  ```

20 Click **Next**.

Specifying exempt IPs

The Exempt IP panel is displayed.

An exempt IP address is a *destination* address for a host or CIDR block behind Symantec Mail Security 8160 for which you do not wish to control SMTP traffic. In contrast, a whitelisted IP address is a *source* address for which you do not wish to control traffic. To whitelist an address or block of addresses, refer to "Uploading whitelisted or blacklisted paths in bulk" on page 64.

Traffic to IPs you provide on the Exempt IPs panel will pass through the 8160 without any lookup or processing, as opposed to IPs you add to the whitelist, which are still looked up and logged before passing through.

21 Add any networks you wish to exempt from processing.
To exempt a single host, add it with a CIDR value of /32.

22 Click **Next**.

Setting up connection shaping

The Connection Shaping panel is displayed.

On this panel, you can specify some options for traffic shaping. You can choose to terminate SMTP connections with any client that attemtps to send data before your mail server indicates readiness.

You can also designate the rejection characteristics when there are no more connections available for blacklisted or regular paths. Choose from TCP RST, SMTP 421, or to drop the connection silently (this option is only available for blacklisted paths). TCP RST sends a TCP reset and drops the connection, whereas SMTP 421 indicates that the service is temporarily unavailable and then drops the connection.

23 Make your selections and click **Next**.

Enabling SNMP data collection

On this panel, you can enable Simple Network Management Protocol (SNMP) by defining a community string and trap destination IP. The trap destination IP is the IP of the machine to which Symantec Mail Security 8160 will send the SNMP events trapped by Symantec Mail Security 8160. The community string is the "password" that you have designated for all SNMP-enabled hosts to use to communicate with the SNMP server. Symantec Mail Security 8160 will trap events related to whether or not the paths database is full. For the SNMP MIB, refer to "SNMP MIB Reference" on page 87.

24 To enable SNMP data collection, check the **Enable SNMP** checkbox.

25 Enter the community string into the **SNMP Community String** field.

26 Enter the IP address of the machine to which the appliance will send trapped SNMP events in the **SNMP Trap Destination IP** field.

27 Click **Next**.

Setting up data synchronization

The Data Synchronization panel is displayed.

28 To set up data synchronization, enter the IP address of Symantec Mail Security 8160 with which you want to exchange data.

If you are configuring for high availability and this is the 2nd machine, specify the IP address of the other Symantec Mail Security 8160 in the cluster.

If you have configured data synchronization, the Key Management panel is displayed, otherwise, proceed to step 30.

29 Do one of the following:

If this is the first of the two Symantec Mail Security 8160 appliances you are configuring for high availability:

- In the **Generate key pair** box, click **Generate**.
  A public/private key pair is generated.
- Download the public and private keys to the machine you are using to access the Control Center and make a note of the location.

If this is the second of the two Symantec Mail Security 8160 appliances you are configuring for high availability:

- Browse for the public and private keys you generated for the first appliance and upload them to this 8160.

30 Click **Next**.

Activating settings

The Activate Settings panel is displayed.

31 Review the values displayed here.

Caution: When you activate the configuration, the 8160 will reboot. When the appliance comes back up, it will start bridging/routing for all protected servers defined. You MUST move the protected servers behind the appliance at this time.

32 If the values are correct, click **Activate**.

Configuring multiple appliances

The most efficient way to configure multiple appliance deployments is to follow the Setup Wizard to configure the first appliance, save that configuration to the machine you are using to access Control Center using the Export Settings option, then log into Control Center on the other appliances and use the Import Settings option to import the same configuration. This will import all the settings you specified for the first appliance, including any public/private key pairs you need for data synchronization. You can then alter the configuration as needed for the subsequent appliances.

To configure multiple appliances

- On the first appliance, once it is fully configured:

1 Using a browser, log into the control center as the admin user.

2 Click **Settings**, then click **Export Settings** in the left hand menu

3 Save the settings file to disk.

- On the second appliance:

4 Initialize the appliance as described in "Initializing Symantec Mail Security 8160" on page 25.

5 Register the appliance as described in "Registering your appliance" on page 26.

6 Log into the Control Center.

7 Click **Settings**, then click **Import Settings** in the left hand menu.

8 Import the previously saved settings.

9 Click **Edit Settings** in the left hand menu.

10 Start the Setup Wizard.
The settings you will have to change are:

- DNS Setup - Hostname

- Bridged vs Routed - if this is a high availability installation, set this system to the secondary appliance.
- Bridged/Routed Configuration Information - change the IP addresses.
- Data Synchronization – delete the current appliance IP address and add the IP address of the first Symantec Mail Security 8160.

11 Activate the configuration.

About configuration

When you complete the Setup Wizard described in "Setting up your appliance" on page 28 and activate your settings at the end, the previously saved settings are backed up, and your new settings are activated.

Exporting a configuration

You can export your current configuration settings to a local file and load them later.

To export your current configuration settings

1 From the Control Center, click **Settings**, then click **Export Settings** in the left menu.
The **Export Settings** page is displayed.

2 Click **Export settings**.
The File Download dialog is displayed.

3 Specify where you'd like to save the configuration settings file, and click **OK**.
The configuration settings file is saved for later use.

Importing an existing configuration

You can import and load configuration settings that you have previously exported using the instructions in "Exporting a configuration" on page 36. The configuration settings file you wish to import must be accessible from the machine you are using to access the Control Center.

To load configuration settings you saved manually

1 From the Control Center, click **Settings**, then click **Import Settings** in the left menu.
The Import Settings page is displayed.

2 Browse for the configuration settings file you wish to load and select it.

3 Click **Import Settings**.

Reverting settings

If you decide not to complete the Setup Wizard, you can revert to the current active settings, throwing away any change you made.

To revert to the current configuration settings

1 From the Control Center, click **Settings**, then click **Revert Settings** in the left menu.
The Revert Settings page is displayed.

2 Click **Revert Settings**.

Synchronizing data between appliances

This procedure assumes that the appliances you are configuring for data synchronization are already up and have been configured using the Setup Wizard. You would normally use this process when configuring synchronization between remote sites.

To set up data synchronization

1 From the Control Center, click **Settings**, then click **Edit Settings** in the left menu, and proceed through the Setup Wizard until the Data Synchronization panel is displayed.

2 Enter the IP address of another Symantec Mail Security 8160 with which you wish this appliance to share network path information and click **Add**.
You can add multiple IPs, one at a time.

3 When you are finished adding IPs, click **Next**.

4 The Key Management panel is displayed.

5 Do one of the following:
If this is the first of the Symantec Mail Security 8160 appliances you are configuring:

- In the **Generate key pair** box, click **Generate**.
A public/private key pair is generated.
- Download the public and private keys to the machine you are using to access the Control Center and make a note of the location.

If you are configuring a subsequent Symantec Mail Security 8160:

- Browse for the public and private keys you generated for the first appliance and upload them to this 8160.

6 Click **Next**.
The Activate Settings panel is displayed.

7 Review the values displayed here.

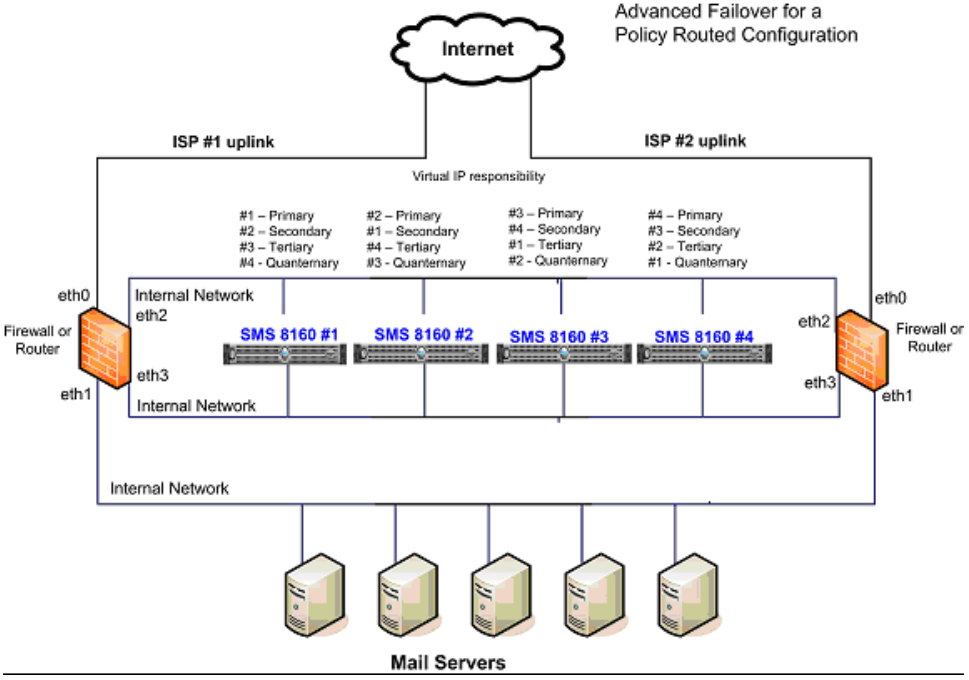
8 If the values are correct, click **Activate**.

The current active configuration is backed up and replaced with the information you have just specified. The appliance reboots.

About advanced failover

Advanced failover allows an appliance to participate as a primary or backup device in up to four clusters of two appliances each. This feature supports transparent failover from failure of up to all but a single member of the group of clusters. It is intended to offer a high level of redundancy in dual-homed, policy routed configurations such as the one shown in Figure 3-1.

Figure 3-1 Advanced failover example



In this implementation, redundant connections from separate Internet Service Providers send email to the Firewall/Routers. Policy routes distribute email

through the four Symantec Mail Security 8160 appliances, where the email streams pass through traffic control before they are sent back through the routers to the mail servers. For more details on this example implementation, refer to "Example advanced failover configuration" on page 41.

Required IP addresses

Each Symantec Mail Security 8160 in an advanced failover configuration requires four IP addresses:

- "Real" IP for Interface 1 – where the Control Center is available
- "Real" IP for Interface 2
- "Virtual" IP for Interface 1 – where incoming SMTP traffic gets forwarded by the router
- "Virtual" IP for Interface 2 – where return SMTP traffic gets forwarded by the router

For a full, four way failover setup, a total of 16 IP addresses are required for the Symantec Mail Security 8160 appliances, plus four for the firewall/router devices.

Virtual IP responsibility level

Each Symantec Mail Security 8160 is assigned a level of responsibility for each of the virtual IP addresses assigned to the cluster. The responsibility level defines the order in which an appliance will take over for a set of virtual IP addresses and respond to ARP requests for that address.

They are ranked in order of priority:

- Primary: assign the virtual IPs to this appliance if it is up
- Secondary: first level backup for a virtual IP
- Tertiary: second level backup for a virtual IP
- Quanternary: third level backup for a virtual IP

Virtual Router IDs

Each set of Virtual IP addresses must be assigned a Virtual Router ID. For each pair of virtual IP addresses set, the Virtual Router ID must be unique to the subnetwork the on which 8160's are located.

Configuring advanced failover

If you have multiple pairs of Symantec Mail Security 8160 appliances and want to configure them for advanced failover, you can edit each appliance's configuration to do so.

To use this feature, all appliances must be operating in routed mode, where each interface of the appliance is on a different IP subnetwork. The policy routes must be defined so that email traffic entering the network through a particular 8160 *must* return to its source through the same appliance.

To set up advanced failover

1. Edit the appliance configuration as described in "Configuring Symantec Mail Security 8160" on page 28.
2. When you reach the **Bridged vs. Routed** panel, select the **Routed** radio button from the **Configuration Type** box and the **Advanced** radio button from the **High Availability** box.
3. Click **Next**.
4. Enter the information for a routed configuration as described in "Setting up virtual bridge or routed configuration" on page 31.
5. Click **Next**.
   If you chose the **Advanced Routes** option on the **Configuration Setup** panel, the **Advanced Routes** panel is displayed.
6. Set up network routes as described in "Setting up network routes" on page 32, and click **Next**.
   The **Advanced Failover** panel is displayed.
   Each of the four columns represents one of up to four clusters.
7. Specify the appropriate internal and external virtual IPs and Virtual Router IDs for the appliance in the context of each cluster.
8. Choose the level or responsibility the appliance has in each of the clusters using the drop-down menus.
   The appliance can serve as the primary, secondary, tertiary, or quaternary failover machine.
9. Click **Next** and proceed through the Setup Wizard until you reach the **Activate Settings** panel, and activate your settings.

Example advanced failover configuration

This section describes the information needed for the example configuration in Figure 3-1.

Using the example, the following Virtual IP addresses will be assigned as the "primary" responsibility of the given appliance:

Table 3-1 Primary virtual IP addresses

8160 unit #	External virtual IP	Internal virtual IP	Virtual Router ID
1	192.168.1.210	192.168.8.210	110
2	192.168.1.211	192.168.8.211	111
3	192.168.1.212	192.168.8.212	112
4	192.168.1.213	192.168.8.213	113

The backup responsibilities are as follows:

Table 3-2 Backup virtual IP addresses

Interface 1 virtual IP	8160 #1	8160 #2	8160 #3	8160 #4
192.168.1.210	Primary	Secondary	Tertiary	Quaternary
192.168.1.211	Secondary	Primary	Quaternary	Tertiary
192.168.1.212	Tertiary	Quaternary	Primary	Secondary
192.168.1.213	Quaternary	Tertiary	Secondary	Primary

The Control Center Advanced Failover Configurations pages for each appliance in this example look like this:

Figure 3-2 8160 #1

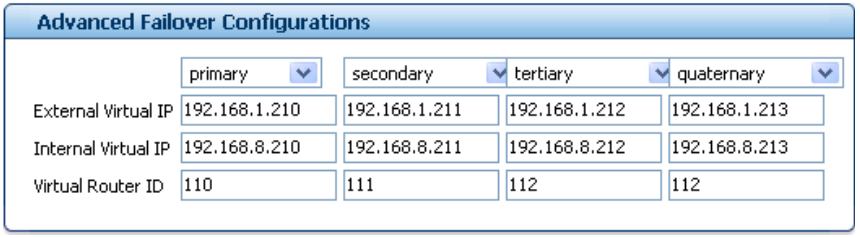


Figure 3-3 8160 #2

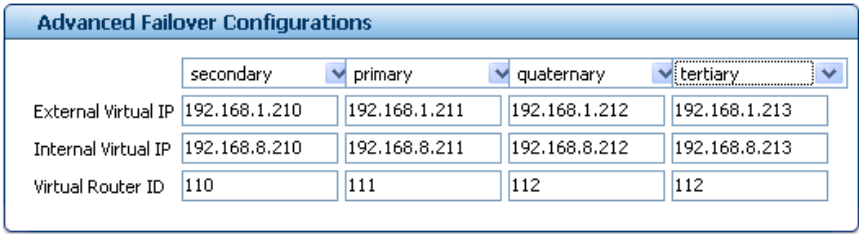


Figure 3-4 8160 #3

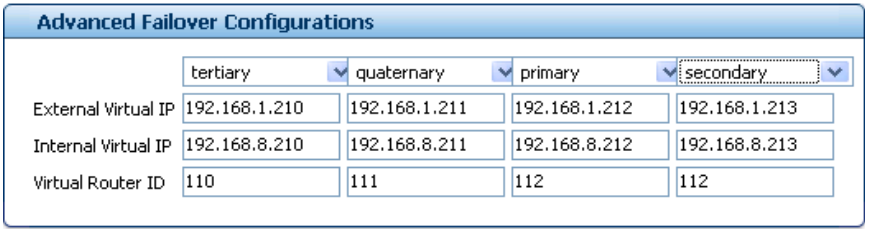
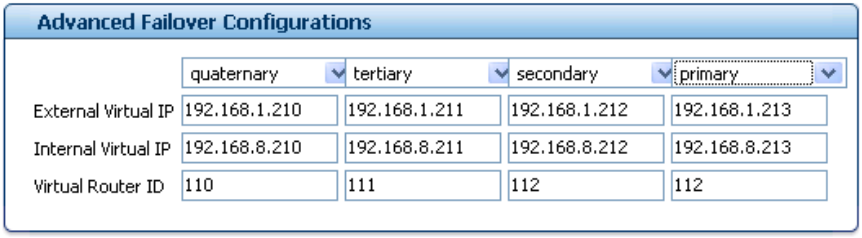


Figure 3-5 8160 #4



Chapter 4

Working with Traffic Control

This chapter includes the following topics:

- About Traffic Control
- Changing Traffic Control levels

About Traffic Control

Traffic Control is how Symantec Mail Security 8160 prevents spam from entering the network by applying TCP traffic and connection shaping to a source network path. Symantec Mail Security 8160 applies traffic and connection shaping based on configuration policy that the administrator can select or manipulate.

Symantec Mail Security 8160 can be in one of three traffic control states:

- Inactive - Incoming email is being passed through the appliance, but is not being analyzed or traffic controlled; refer to "Stopping services (switching to Inactive mode)" on page 68.
- Passthrough - Incoming email is sampled and the spam rating for each path is updated, but no traffic control is applied.
  This is the default state for the 8160 when first configured. It is recommended that the appliance remain in this state for a minimum of 24 hours to get a representative sample of the incoming email traffic before switching to "active" mode.
- Active – Incoming email is sampled and the spam rating for each path is updated. Quality of service, including allowed bandwidth, concurrent connections, messages per connection and reconnect timeout (connection frequency), is enforced.

The real time status of traffic control is displayed in the Control Center at the top right side of the page.

There are some systems that you should consider whitelisting immediately:

- Other internal SMTP servers that send mail to your systems
- Systems on the External side of the 8160 that monitor your protected mail servers. These systems typically connect to the SMTP server and then immediately quit the conversation. Since they never send a mail message, they fall into the “default” category which limits the number of concurrent connections and number of connections per se cond they are allowed. This could trigger false “down” alerts.

Changing Traffic Control levels

You must have System or Master Administration privileges to change the Traffic Control level of the 8160.

Changing Traffic Control to Passthrough mode

Setting Symantec Mail Security 8160 to Passthrough mode allows it to sample incoming traffic and “learn” about your site’s traffic shaping needs.

To set the appliance to Passthrough mode

1. From the Control Center, click **Administration**, then click **Traffic Control** in the left menu.
2. Select the **Switch to Passthrough** radio button.
3. On the Confirmation page, click **Yes**.

Changing the level of active control

Traffic Control is normally applied in stages, to allow for analysis of the effect it has on the incoming email stream. When you initially activate the 8160 Traffic Control, it is at Stage 1. When you are satisfied that the appliance is working correctly, you can increase the Traffic Control level to Stages 2 through 5.

To change the Traffic Control stage

1. From the Control Center, click **Administration**, then **Traffic Control**. The Traffic Control page is displayed.
2. Select the radio button for the Traffic Control stage you want to activate. Higher numbers indicate more control.

3 Click **Activate**.

Tuning Traffic Control manually

You can manually tune aspects of Symantec Mail Security 8160 Traffic Control configuration by editing the configuration files.

Warning: Manually editing the traffic control files is normally unnecessary. Changes to traffic control must be made with extreme caution as undesirable results may occur if these parameters are not configured properly.

To edit a Traffic Control configuration file

1 From the Control Center, click **Administration**, then **Traffic Control**.
The Traffic Control page is displayed.

2 Select the **Custom** radio button and click **Edit Custom**.
If you have already customized one or more Traffic Control configuration files, you can select the one you want to edit from the drop-down menu.
The Edit Traffic Control page is displayed.

3 Select the radio button for the Traffic Control configuration file you want to edit, and click **Edit**.
You can use an existing Traffic Control configuration file as a template for a custom configuration file by either:

- Downloading it and saving it with a new filename and then re-uploading it using the Upload Configuration File functionality, or
- Selecting it for editing and then renaming it on the Edit page.

The Edit Traffic Control page is displayed.
The Classification column lists the breakdown of spam percentage ratings for which traffic control is configurable. There are control levels for default (or unknown) paths, and for paths that are 0-3% spam, 4-10% spam, 11-50% spam, etc.
The rest of the columns define parameters that are configurable for each of the Classification ratings.
The following are configurable values:

- Threshold – The minimum number of messages that must be received from a path before it will be included in this classification level. If fewer messages have been received, the path will be included in the next most appropriate classification. For the best classification level, this means that connections will be shunted into the next worse level. For all other classification levels with a threshold value, a connection not meeting the specified threshold

will be shunted up the levels until it satisfies a classification level's threshold value. All source network paths satisfy the threshold value for a level that has no threshold allocated.

- Connection Limit – The total number of simultaneous connections allowed for all paths at this classification. Connections that are evaluated to belong in one classification level will be shunted to the next lower level if the classification level has no more available conections. In this case, the connection will be treated to the same resource limits as any of the classification level's other connections.
- Bandwidth – The total bandwidth in kilobits/second allowed for all paths at this classification. A connection will receive a bandwidth allotment equal to the total bandwidth in its extant classification level divided by the connection limit for the classification level. You can specify bandwidth with this in mind, or you may find it more appropriate to think about the total message ingress into your network when setting this figure.
  Table 4-1 shows an estimate of the relationship between the kilobits/second value and the number of 10kb messages per hour. For example, to limit a certain message classification to approximately 40 messages per hour, set kbits/s to 1.

Table 4-1 Estimated kbit/second per messages/hour

kbit/s	msgs/hour
1000	40500
800	32400
700	28350
600	24300
500	20250
250	10125
100	4050
50	2025
10	405
8	324
7	283
6	243
5	202

Table 4-1 Estimated kbit/second per messages/hour

kbit/s	msgs/hour
4	162
3	121
2	81
1	40
0.9	36
0.8	32
0.7	28
0.6	24
0.5	20
0.4	16
0.3	12

- Connections/IP- The maximum number of simultaneous connections per path allowed. Subsequent connection attempts by a path after it reaches this limit will be rejected as long as all of the previous connections are still open.
- Msgs/Connection – The maximum number of messages per connection from a path allowed. When a source attempts to send more messages in a single connection, the connection is closed by Symantec Mail Security 8160.
- Connection Timeout – The number of seconds that connection attempts from a given path will have to wait before they can reconnect after a path has met its Connections/IP value. The timeout is applied from the beginning of each connection. Connections attempted from a path before the timeout has expired will be rejected.
- Overflow Bucket –This radio button allows you to select which classification to apply to connections from new paths when Default is full. When Default has no more available connections to allocate, the Overflow Bucket indicates the classification level that will be examined first when looking for an available connection slot. If that level is also full, examination continues as described above.

4 To edit a value, select its current value and type in the new value.

5 When you have finished editing, click **Save**.
The Traffic Control page is displayed.

6 To activate the configuration you just edited, select its radio button and click **Activate**.
Your new configuration is activated.

Chapter 5

Working with graphs and reports

One of the most useful features in the Control Center is the ability to view and report on operational and statistical information related to your Symantec Mail Security 8160 installation.

This chapter includes the following topics:

- Viewing current path statistics
- Viewing available graphs
- Modifying graph display and saving graph data
- Viewing overall path statistics
- Viewing System Status
- Viewing the Event Log
- Viewing email traffic estimates
- Viewing overall performance
- Viewing and creating reports

Viewing current path statistics

When you log into Symantec Mail Security 8160, you see the Current Statistics page. You can also see this view when you click the Status tab.

This page gives a live, dynamically updated dashboard of clickable mini-graphs that show path quality, CPU utilization, message load, and bandwidth utilization. To see larger, more detailed views of each graph, click on the graph itself.

The current Path Quality graph provides a live view of the breakdown of message quality. The green line denotes messages that have a 0% - 10% likelihood of being spam. The yellow line denotes messages that have a 11% - 75% likelihood of being spam. The red line denotes messages that have a 76% - 100% likelihood of being spam. The gray line denotes messages from paths which have not been classified yet.

Information is also provided about the number of connections, how much bandwidth (in Kbits) is being used, the message load in messages per minute, and the path quality, described as ‘clean’, or ‘mixed’, and the number of spam messages per minute.

Viewing available graphs

The **Status** section provides both current and historical information about the operations of your Symantec Mail Security 8160 installation in graphical form. This section describes the following available line graphs:

- Connection load graph
- Bandwidth utilization graph
- Message load graph
- Path quality statistics graph
- CPU utilization graph

Along with the graphical data, a table of the data points used to build the graph is also displayed beneath each graphical representation.

To view current statistics and historical data in graph form

- From the Control Center, click **Status**, then click the name of the graph you would like to see in the menu on the left.

Connection load graph

The connection load graph shows the total number of paths that were connected to your network at each point in time.

Bandwidth utilization graph

The bandwidth utilization graph displays the amount of overall bandwidth used by your network connections expressed in Kbits per second.

Message load graph

The Message Load graph, shows the overall rate of messages per minute that have been allowed into your network over time.

Path quality statistics graph

The path quality statistics graph shows Symantec Mail Security 8160's analysis of the quality of messages that have been sent from various paths into your network. The graph has four color-coded lines to illustrate different classes of messages:

Green	Messages with a 0 to 30% likelihood of being spam (clean).
Yellow	Messages with a 11 to 75% likelihood of being spam (mixed).
Red	Messages with a 76 to 100% likelihood of being spam (spam).
Gray	Messages that have not yet been classified.

The graph shows both the historical 24-hour data as well the current clean, mixed, and spam messages/minute.

CPU utilization graph

This graph shows the percentage of CPU in use on the Symantec Mail Security 8160 over time.

Modifying graph display and saving graph data

Each of the graphs can be modified to suit the time range that you would prefer for your reporting purposes. Additionally, you can export the data points used to construct the graphs in comma separated values (CSV) format for use in your own customized reporting or graphing applications.

Changing the graph time frame

You can change the time frame (and corresponding graph scale) of the data points that comprise the graph. You can choose to view a graph versus any one of the following graph time frames:

- Partial Day
- Day
- Week
- Month
- Year
- 10 years

To change the time frame of a graph

- On the graph page, in the timeframe drop-down box, select the new time frame.
  The graph and corresponding data table update automatically.

Exporting the graph data

You may also export the data table used to create the graphs in the Statistics page, in comma separated variable (CSV) format. This data may be imported into spreadsheet, database, or reporting programs for customized graphing and/or reporting.

To export graph data

1. Below the graph, click **Download this graph's data**.
2. In the location text box, type the location where the .csv file should be saved.
3. To import the CSV file into another program, consult that program's documentation or help files.

Viewing current network statistics

The Current Network Information page contains the following three fields of information regarding the router and its role in your network:

- External network
- Protected network
- ARP table

To view network statistics

- From the Control Center, click **Status**, then click **Network Statistics** in the menu on the left.
  The Network Statistics page is displayed.

External network

The External network field contains information about the interface from the appliance to the external internet. The first part of the table shows packet volumes and error information for packets received and transmitted. This information may be useful in investigating network connectivity issues.

The configuration information for the interface is displayed in the second table.

Protected network

The Protected network field describes the interface from the appliance to the protected network (where your protected SMTP server is located). The first part of the table shows packet volumes and error information for packets received and transmitted. This information may be useful in investigating network connectivity issues.

The configuration information for the interface is displayed in the second table.

Arp Table

This table shows the contents of the ARP cache on the appliance and the interface the entry is located on.

Viewing System Status

The System Status page displays summary and detail status of the appliance, including System Uptime, Load Average, Rule updates, Software update availability, BRS updates, Path database backup and Failover status.

To view System Status

- From the Control Center, click **Status**, then click **System Status** in the menu on the left.
  The System Status page is displayed.

Viewing the Event Log

The Event Log displays all administrator actions and alerts issued.

To view the Event Log

- From the Control Center, click **Status**, then click **Event Log** in the menu on the left.
  The Event Log page is displayed.

Viewing overall path statistics

The Path Statistics page contains a table that shows a detailed breakdown of the classifications of all network paths that have sent email into your network. As email traffic enters your network, the 8160 analyzes the traffic originating from that network path and assigns a classification to that path based on the appliance's determination of the likelihood that it is sending spam into your network. The lower the percentage, the less likely spam is being sent on the specific path.

To view classifications of network paths

- From the Control Center, click **Reports**, then click **Path Statistics** in the menu on the left.
  The Path Statistics page is displayed.

The Path Statistics page provides the following information about classifications of network paths:

Table 5-1 Path Statistics page information

Column	Description
Path Classification	Shows the categorization of the approximate spam received from various paths.
Number of Paths	Shows the total number of paths known to be producing the levels of Spam seen in column 'Path Classification'.
Percentage Total	Shows the percentage relative to the total amount of email traffic going through Symantec Mail Security 8160.

Figure 5-1 shows an example of detail from the Path Statistics page.

Figure 5-1 Path Statistics page detail

This detail shows that 90% - 100& of the mail from these 540 paths has been is spam, and make up 70.4% of all paths stored in the database.

The Path Statistics page also displays the total number of network paths that are known to be sending email traffic into your network as well as a time stamp showing the time this information was last updated.

Viewing email traffic estimates

The email traffic graph shows emails that have been processed, and their projected amounts in the future, based on data collected while the appliance is in passthrough mode.

Note: At least one day's worth of e-mail with the appliance in passthrough mode is required to generate this graph.

Once Symantec Mail Security 8160 has been placed in Active mode, this graph should no longer be referenced. Instead, use the Overall Performance graph described in Viewing overall performance.

To view email load estimates

- From the Control Center, click **Reports**, then click **Email Estimates** in the menu on the left.
  The Email Estimates page is displayed.

Viewing overall performance

The Performance page contains a graph that shows your email volume before and after implementing Symantec Mail Security 8160. This graph assumes that the rate of Spam increases at 10% per month. The performance graph is not available until three weeks worth of data has been collected.

To view overall performance

- From the Control Center, click **Reports**, then click **Performance** in the menu on the left.

The Performance page is displayed.

A figure of 10% is used because statistical data shows that on average, spammers will increase their mail by this amount each month in their attempts to bypass antispam technology.

Viewing and creating reports

Using the Control Center, you can view and download the data from a number of preconfigured reports or create custom reports.

The following preconfigured reports are available:

- Path Quality (RCPTs)
  A RCPT is when an e-mail is sent to a unique recipient. This graph shows how many RCPTs were received per second, and breaks them down based on the quality of the path.
- Path Quality (Complete Transactions)
  A complete transaction is when a complete email is sent successfully. This graph breaks down the number of complete transactions per second based on the quality of the graph. The difference between a complete transaction and a RCPT is that the sending machine may break off the connection before they finish sending the message. This graph only shows messages that were successfully sent.
- Transaction Activity
  This graph plots the following:
  - The number of SMTP transactions per second across all paths. SMTP Transactions can each include one or more RCPTs.
  - The number of RCPTs seen per second across all paths
  - The number of messages that were properly ended.

  This graph can be used to determine if there are an abnormal number of messages that were not ended properly, OR if (on average) there is more than one recipient per message.

To display a preconfigured report

1. From the Control Center, click **Reports**, then click **View Reports** in the menu on the left.
   The View Reports page is displayed.
2. Select the report you wish to view from the **Report** drop-down list, select the timeframe for which you wish to generate the report from the **Timeframe** drop-down list, and click **Generate Report**.

3 The report is generated.

To create a custom report

1 From the Control Center, click **Reports**, then click **Custom Reports** in the menu on the left.
The Custom Reports page is displayed.

2 From the **Classification** column, select a classification of data to graph from the first drop-down list.

3 From the **Data Source** column, select a source of data to use from the drop-down list.
For a description of each data source, refer to "Data sources for custom reports" on page 57.

4 From the **Color** column, specify the color line you want this data displayed in.

5 From the **Dates** column, specify the start and end dates for your report by clicking on the dates and selecting from the popup calendar.

6 Repeat steps 1-4 as needed for additional data sources and classifications.

7 If you need more than four sources, click **Add Row**.

8 When you have specified all the sources of data for the report, click **Generate Report**.
The report is generated.

To export report data

1 Below the report, click **Download this graph's data**.

2 In the location text box, type the location where the .csv file should be saved.

3 To import the CSV file into another program, consult that program's documentation or help files.

Data sources for custom reports

The following is a list of the data sources available for use in custom reporting.

- Connection Attempts
  The number of connections to protected servers that were attempted , regardless of whether or not they resulted an an established connection.
- Connections Made
  The number of SMTP connections to protected servers that were actually established.

- Messages Seen
  The number of the SMTP transactions that were observed by Symantec Mail Security 8160. This is not the same as the number of messages delivered to end users, as the protected server may bifurcate messages after Symantec Mail Security 8160 is no longer involved in the transaction. Additionally, SMTP transactions with multiple recipients are only counted once for this metric.
- Ends of mails
  The number of SMTP transactions that were observed actually attempting to send mail. Examples of transaction ending events are the MAIL command after a previous transaction, an RSET command, a QUIT command or a connection tear down following an SMTP transaction. This does not include the number of RFC 2821 MAILEND sequences seen; this metric is described in the Message Endings data source.
- Recipients Seen
  The number of recipients seen during SMTP transactions. This metric is closer to the actual number of email messages received by end users but does not take into account refusal of recipients by the protected servers.
- Message Endings
  The number of SMTP transactions that were terminated specifically with an RFC 2821 MAILEND sequence (such as `<CR><LF>.<CR><LF>`).
- CPU Utilization
  The average load on the CPU at timed intervals on a range from 0 to 10 (0 meaning idle, 10 meaning the maximum load).
- Bandwidth
  The amount of bandwidth Symantec Mail Security 8160 uses to forward SMTP traffic.
- Blacklist Rejected
  The number of connections that were refused because their sources were blacklisted by an Administrator.

Chapter 6

Working with network path information

This chapter includes the following topics:

- About network path information
- Searching network path information
- Modifying network path information
- Making bulk changes to network paths
- Uploading whitelisted or blacklisted paths in bulk
- Maintaining the paths database
- Backing up path data
- Restoring path data

About network path information

Symantec Mail Security 8160 works by analyzing your network's mail flow and identifying the behavior of various network paths over time. All of this happens transparently, without the need for administrative intervention. You may want to make changes in response to current conditions.

If you are a Data or Master Administrator, you have access to these path administration functions:

Altered Paths Page	Add or edit network paths considered to be spam.
Changelog	View the change log; an audit trail of all manual changes made by all appliance administrators.

Searching network path information

The Search function gives you easy access to network path information.

To search historical path data and its associated spam categorization, you must know the domain name, Classless Internet Domain Routing (CIDR) block or IP address of the network path. Table 6-1 defines the search parameters.

Table 6-1 Network path search parameters

Search parameter	Format	Search results
IP Address	192.168.1.100	Paths originating at the host with IP address 192.168.1.100.
Domain Name	fflanda.com	Paths originating from IP addresses that resolve to the MX record for domain name fflanda.com.
CIDR Block	192.168.1.0/24	Paths originating from hosts in the subnet denoted by the class C address 192.168.0.0 (for example 192.168.1 ... 192.168.1.0.255)

To search network path information

1. From Control Center, click **Paths**.
2. The Search/Modify Paths page is displayed.
3. Enter one of the following:
   - IP Address
   - Domain Name
   - CIDR
4. Click **Search**.

Note: You can also use the Path Search field on every page in the Control Center.

For each network path returned by the search, the approximate spam rate and path confidence are displayed. The spam rate is expressed as an approximate percentage of traffic from that path which is spam. The path confidence indicates how confident Symantec Mail Security 8160 is in its analysis of that path.

- WL: Whitelisted
- BL: Blacklisted

- AA: Administratively Altered
- RM: from a Remote Machine in the cluster
- BRS: listed in the Brightmail Reputation Service
- BEIK: from a client customized using the Brightmail Engine Integration Kit
- LOCK: from a path for which you have specified a spam rating and locked (refer to "Modifying network path information" on page 61).

In some cases, the spam rate and path confidence are not displayed, but a single value is shown to express the status of that path. These special values are:

Unknown	No path data is available because insufficient traffic has been sent from that path to make a valid determination or the path information has been administratively deleted.
Whitelisted	The path has been administratively configured such that this path is being treated as a non-spam sending path.
Blacklisted	The path has been administratively defined such that it is considered to be a spam sending path.

If you use the Search Box to navigate to a path, you can make your changes directly from the Search Results page, if a single result is returned. If multiple results are returned, you can perform bulk modifications on all results returned, or you can change path information using the Path Administration page.
See "Making bulk changes to network paths" on page 63. See "Modifying network path information" on page 61.

Modifying network path information

You can view, add or edit information about paths that you consider to be spam.

A key function of Symantec Mail Security 8160 operation is the analysis, over time, of email traffic from various network paths. This analysis is done and the results acted upon automatically, without any administrator intervention. However, certain situations may arise where you want to override settings and manually configure information about specific network paths.

You can change path information in one of the following ways:

Altered Paths page	Make changes to network paths that you or another administrator in your organization have already manually configured.
Search Results page	Make changes to a network path based upon a hostname, domain name, IP Address or IP CIDR block address.

To modify a network path

1 In the Control Center, click **Paths**.

2 Either:

- Search for the path you want to alter using the Search/Modify Paths page using the information in "Searching network path information" on page 60 and click on it.
- Locate the path on the Altered Paths page and click on it.

The Editing page is displayed.

3 If you want to add this path to the Whitelist or Blacklist, click the appropriate button.

The path is immediately added to the specified list.

- When a network path is administratively set to Blacklisted, Symantec Mail Security 8160 refuses all connections from that path.
- When a network path is administratively set to Whitelisted, Symantec Mail Security 8160 gives maximum quality of service to connections from that path.

4 If you want to erase the recorded history for this path, click **Erase Path**.
The history for this path is immediately erased. When you erase the recorded history of a path, the appliance's prior analysis of that path is discarded. It will start again as traffic from that path is analyzed in the future.

5 If you want to lock this path, click the **Lock** checkbox.
If this path is already in the Whitelist or Blacklist, locking it will have no effect.

6 When you are finished, click **Update**.

Changing a path's assumed spam rate

You can change a path's assumed spam rate manually from 0% to 100% spam to adjust how you want Symantec Mail Security 8160 to treat that specific path. This produces results as though the appliance were making its own conclusions about that path based on analysis over time, but with immediate results.

You may want to use this option to pre-configure Symantec Mail Security 8160 with information about paths it has not yet seen, or you may choose to override the appliance's analysis based on information you may have about a network path.

To change a path's assumed spam rate

1 In the Control Center, click **Paths**.

2 Either:

- Search for the path you want to alter using the Search/Modify Paths page using the information in "Searching network path information" on page 60 and click on it.
- Locate the path on the Altered Paths page and click on it.

The Editing page is displayed.

3 Select the new spam rate from the drop down list.

4 If you want to lock this path, click the **Lock** checkbox.
Locking the path prevents other processes such as the Symantec Mail Security 8160 analysis module from updating the value for the path.

5 Click **Update**.

Viewing manually altered paths

The Altered Paths page shows all network paths that have been manually changed by Data or Master Administrators.

To view a manually modified path

- In the Control Center, click Administration, then click **Altered Paths**.
The Altered Paths page is displayed. You can edit a path by clicking on that path's entry in the table.

Making bulk changes to network paths

There may be times when you want to make changes to a number of network paths simultaneously. You can do this from any Search Results page where multiple results have been returned (for example, when your search criteria was a domain name or CIDR block).

You can use the following commands to make bulk changes to all network paths listed on the page:

Whitelist All	Mark all paths listed in the results table as 'whitelisted'.
Blacklist All	Mark all paths listed in the results table as 'blacklisted'.
Erase All	Erase analysis data for all paths listed in the results table.

To make bulk changes to network paths

1 In the Control Center, click **Paths**.

2 In the Search text box, type one of the following:

- IP Address
- Domain Name
- CIDR

3 Click **Search**.
Review the results of the search to make sure you want to apply bulk changes.

4 In the right pane, click one of the following options:
- Whitelist All
- Blacklist All
- Erase All

Uploading whitelisted or blacklisted paths in bulk

You may have lists of network paths that you want Symantec Mail Security 8160 to automatically allow or disallow traffic from without doing any processing. You can upload whitelisted and blacklisted sender lists if you are logged in as a Data or Master Administrator.

The files you upload must be plain text and can contain individual IP addresses or CIDR blocks, one IP or CIDR block per line.

To upload allowed or blocked sender lists

1 In the Control Center, click Paths, then click on **Bulk Path Upload**.
The Bulk Path Upload page is displayed.

2 From the appropriate section, browse for the file you wish to upload.

3 Click the **Upload** button for the type of list you're uploading.
The file is uploaded to the appliance.

Maintaining the paths database

You may from time to time wish to prune back the number of altered records in the paths database. You may have received an alert notifying you that the database is at capacity, or you may wish to simply reset the number of administratively altered records to 0.

To delete all administratively altered paths

1 In the Control Center, click **Paths**, then click on **Database Maintenance**.
The Database Maintenance page is displayed.

It is strongly recommended that you back up your database before deleting all administratively altered records. Use the Backup utility to do so, described in "Backing up path data" on page 65.

2 When you have backed up your data, click **Delete All Administratively Altered records**.

3 The records are deleted.

Backing up path data

You can back up the database that stores all administratively altered path records to disk.

To back up the database

1 From the Control Center, click **Paths**, then click **Backup Path Data** in the menu on the left.
The Backup Path Data page is displayed.

2 Click **Backup Now**.
The Save dialog for your system is displayed. If you have no administratively altered path data to back up, you will see a message indicating this.

3 Choose where you'd like to save the backup file and save the file.

Restoring path data

You can restore the database of administratively altered paths from a file to which you backed up earlier. To do this, you must be able to browse to the backup file from the machine you are using to access the Control Center.

To restore the database

1 From the Control Center, click **Paths**, then click **Restore Path Data** in the menu on the left.
The Restore page is displayed.

2 Browse for the backup file you made and select it.

Note: Only paths that have been administratively altered will be restored. If a path already exists, it will be overwritten. If a path in the file does not exist, it is added to the database.

Chapter 7

Administering Symantec Mail Security 8160

This chapter includes the following topics:

- Starting, stopping, or powering down
- Viewing the Changelog
- Administering user accounts
- Troubleshooting
- Software updates from Symantec
- Setting up alerts
- Managing Licenses

Starting, stopping, or powering down

You can temporarily disable the antispam services of Symantec Mail Security 8160, or shut it down to prepare for a move or for physical maintenance.

When Symantec Mail Security 8160 is first installed, it comes up in Passthrough mode, where no traffic control is applied. In Passthrough mode, the appliance examines mail from source Paths (IP addresses), rating the mail as to the probability it is spam, and recording the results for each Path in the internal database.

You can switch from Passthrough mode to Inactive mode for diagnostic purposes.

Stopping services (switching to Inactive mode)

You must be logged on as a Master or System Administrator to deactivate the antispam services of Symantec Mail Security 8160.

Once you have stopped services, the status indicator in the upper right of the page displays the word **Inactive** in red. This status remains on all pages, for all user accounts, until Symantec Mail Security 8160 is started again.

Note: While services are Inactive, you cannot alter paths or perform any action other than manipulate the configuration. Graphs will no longer be updated and the paths database is inaccessible.

To stop Symantec Mail Security 8160 services

1. From the Control Center, click **Administration**.
2. In the right pane, under Adjust Appliance State, click **Turn Off**.
3. On the Confirmation page, click **Yes**.
   If you do not want to deactivate filtering services, do one of the following:
   - Click **Cancel.**
   - On your browser, click **Back**.

You also can completely power down the appliance. See "Powering down and rebooting the appliance" on page 69.

Starting services (switching to Active mode)

You can reactivate Symantec Mail Security 8160 antispam services after they have been manually stopped. Once the appliance is reactivated it will resume analyzing email sources and reducing spam.

To start Symantec Mail Security 8160 services

1 From the Control Center, click **Administration**.

2 In the right pane, under Adjust Appliance State, click **Switch to Active**.

Powering down and rebooting the appliance

You can power down Symantec Mail Security 8160 in preparation for moving, network maintenance, or other situations that require that it be powered off. You can also reboot the appliance.

To power down or reboot Symantec Mail Security 8160

1 From the Control Center, click **Administration**.

2 In the right pane, under Power Appliance Down, click **Power Down**.

3 If you want to reboot the appliance, click **Reboot**.

Viewing the Changelog

Symantec Mail Security 8160 maintains an audit trail of manual changes made by all administrators in a change log. If you have Data or Master Administrator privileges, you can view the audit trail.

The Changelog lists all changes made by Data and User Administrators using the Control Center as well as the time the change was made.

To view the Changelog

- In the Control Center, click **Administration**, then click on **Changelog**. The Changelog page is displayed.

Note: You can also use this page to make manual path changes by clicking on any path shown in the Action Taken column of the table.

Administering user accounts

You can use the Control Center to set limits on the functions that specific users can perform by assigning them to administrative groups which have defined roles:

Basic User	Read only access to data; can only change own password.

Data Administrator	Can modify the Path data stored on the appliance.
User Administrator	Can add, delete, and modify user accounts.
System Administrator	Can turn the appliance on and off.
Master Administrator	All the above privledges,, and can change the configuration settings of the appliance

To administer user accounts

- From the Control Center, click **Administration**, then click **User Administration** in the left menu.
  The User Administration page is displayed.

On this page, a set of tables display information about each user name, group and role defined in the system.

Changing a user password

The User Administration page lists each active user. You must first select a user before changing their credentials. You must have User Administrator privileges to change another user's password.

To change a user password

1. On the User Administration page, in the Users table, select the radio button next to the user name whose password you want to change and click **Edit.**
   The User Info page is displayed.
2. In the **Password** text box, type the new password.
3. In the **Confirm** text box, retype the new password.
4. Click **Apply Changes.**
   The password is changed.

Caution: Document the administrator password and store it in a safe place.The administrator password can not be reset if it is lost.

Adding a new user account

You must be a User Administrator or Master Administrator to add a new user account. Adding a new user account allows a that user to access the Control Center.

To add a new user account

1. From the Control Center, click **Administration**, then click **User Administration** in the left menu.
   The User Info page is displayed.
2. At the bottom of the Users box, click **New User**.
   The New User page is displayed.
3. In the **User** name text box, type the user name of the new user.
4. In the **Password** text box, type a password for the new user.
5. In the **Confirm** text box, retype the password for the new user.
6. Under **Member Groups**, check the group(s) to which you want to assign the new user.

Note: To define a read-only user, leave all Member Groups unchecked.

---

7. Click **Apply Changes.**

Deleting a user account

Deleting a user's account means that they will no longer have access to the Control Center. You must be a Master or User Administrator to delete a user account.

Note: You cannot delete the Admin user account.

To delete a user account

1. In the Control Center, click **Administration**, then **User Administration**.
   The **User Administration** page is displayed.
2. In the **Users** box, select the checkbox next to the name of the user you wish to delete.
3. Click **Delete**.
4. Confirm the deletion.
   The user account is deleted.

Modifying an existing user account

Existing user accounts can be modified to change the group/role membership of the user or their password. You must be a Master or User Administrator to modify an existing user account.

To modify an existing user account

1. In the Control Center, click **Administration**, then **User Administration**.
   The User Administration page is displayed.
2. In the **Users** box, select the checkbox next to the name of the user you wish to modify.
3. Click **Edit**.
   The User page for this user is displayed.
4. If you want to change the user password,
   - In the **Password** text box, type the modified password of the user.
   - In the **Confirm** text box, type the modified password of the user.
5. If you want to change the groups to which this user belongs, under **Member Groups**, check the groups to which you want to assign the user.

Note: To define a basic user, leave all Member Groups unchecked.

---

6. Click **Apply Changes.**

Troubleshooting

The troubleshooting page allows you to test network connectivity to protected servers. Two tools are available, `ping` and `traceroute`. `ping` is most useful in virtual bridge mode or when Symantec Mail Security 8160 is acting as the router for the subnet on which the mail server(s) is located. `traceroute` is useful when the protected server is located behind another device such as a router.

Software updates from Symantec

You can view your current system software version and, if available, request software updates.

To View the current software version or request an update

1. In the Control Center, Select **Administration**, then click **Software Updates**.

The newest versions of software, if newer than your installed version, are displayed with a checkbox and with a status of **Available**.

2 If you wish to install new software, check the box next to the available software version you want to install and click **Update**.
The appliance will download the new software, update your existing installation, and then reboot. This may take a few minutes. During this time, you will not have access to the Control Center. When the system has rebooted, re-log into the Control Center and proceed.

Setting up alerts

You can specify up to 10 email addresses to which Symantec Mail Security 8160 will send alert notifications.The addresses you specify cannot be local to the appliance host.

The 8160 will send out the following alerts for the stated conditions:

- The appliance database is full; please prune the records.
  This alert is sent when the paths database reaches the maximum allowed number of records.
- The appliance database is no longer full.
  This alert is sent when the paths database was full but has been pruned.
- The appliance disk is at 90% capacity.
  This alert recommends that you use the CLI `clear` command to empty log files in order to recover disk space. Refer to "clear" on page 82 for information.
- The appliance has lost contact with other cluster member(s).
  This alert is sent when one or more of the connections to other appliance cluster members breaks off.
- The appliance has reestablished contact with other cluster member(s).
  This alert is sent when a previously broken connection to a cluster member is reestablished.
- A software upgrade is now available for installation.
  This alert is sent when a software upgrade is available for download/ installation.

To specify email addresses to the alert list

1 From the Control Center, click **Administration**, then click **Alert Setup** in the menu on the left.
The Alert Setup page is displayed.

2 Enter the email address to which you want the alerts to be sent.
If there is more than one address, separate them with commas.

3 Enter the name of your SMTP server in the **Smart-Relay Host** field.

4 If the SMTP server requires username and password, enter them in the **Account** and **Password** fields.
The supported SMTP authentication method is CRAM_MD5.

5 Click Set **Alert.**

Managing Licenses

To view and add licenses

1 In the Control Center, Select **Administration**, then click **Licensing**.

2 Review the license information.
Next to each feature to which a license can apply, a start date and expiration date is shown.

3 To license a particular feature, either paste in a license key from an email you have received from Symantec, or browse for a filename in the Install a new license file box.
If you have licenses for other Symantec products in the same location, be sure you have selected the correct license before proceeding.

4 Click **Install**.

Appendix A

Example Deployment Scenarios

This Appendix contains examples of various potential deployment options for Symantec Mail Security 8160, with information about how to implement Symantec Mail Security 8160 within the depicted network infrastructures.

- High availability virtual bridge implementation
- High availability router implementation
- Mail server gateway router implementation
- Policy routed router implementation

High availability virtual bridge implementation

The diagram below shows an installation of two Symantec Mail Security 8160 appliances in virtual bridge mode, configured for high availability. In this configuration, the appliance designated as the primary appliance provides data synchronization to the secondary appliance. If the primary appliance is removed from service, the traffic flows to the secondary appliance, which has up-to-date configuration and path information. The instructions in "Setting up your appliance" on page 28 explain how to deploy two Symantec Mail Security 8160 appliances in this configuration.

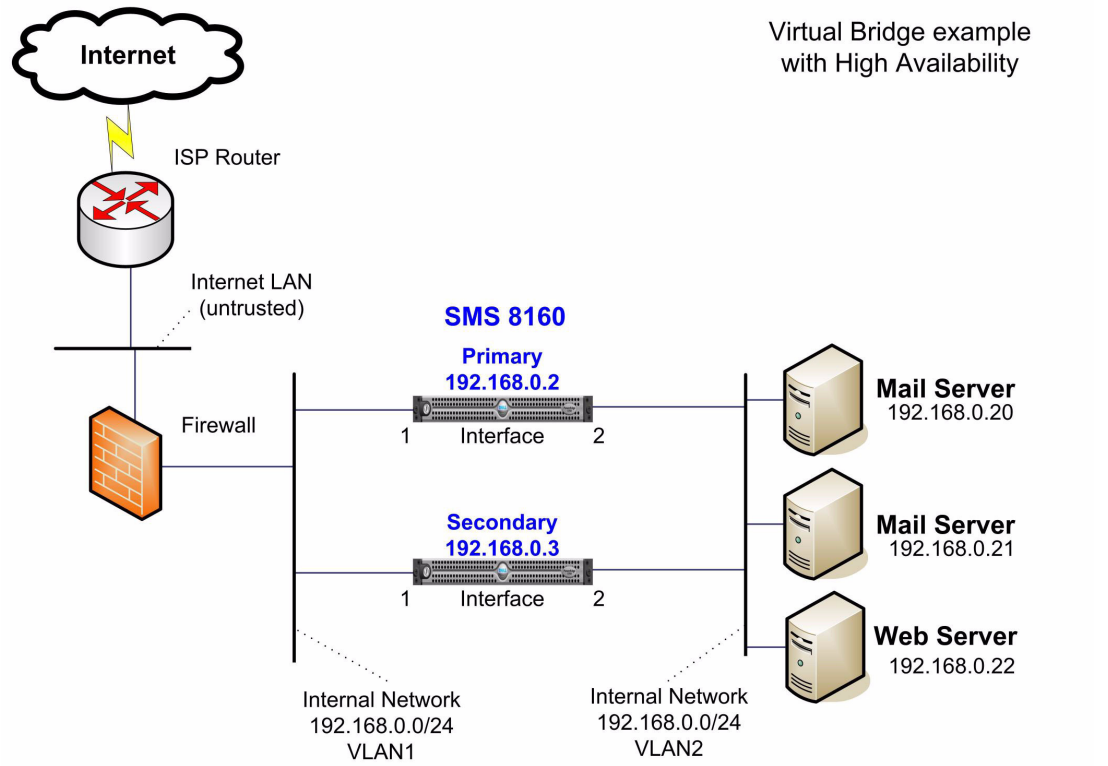
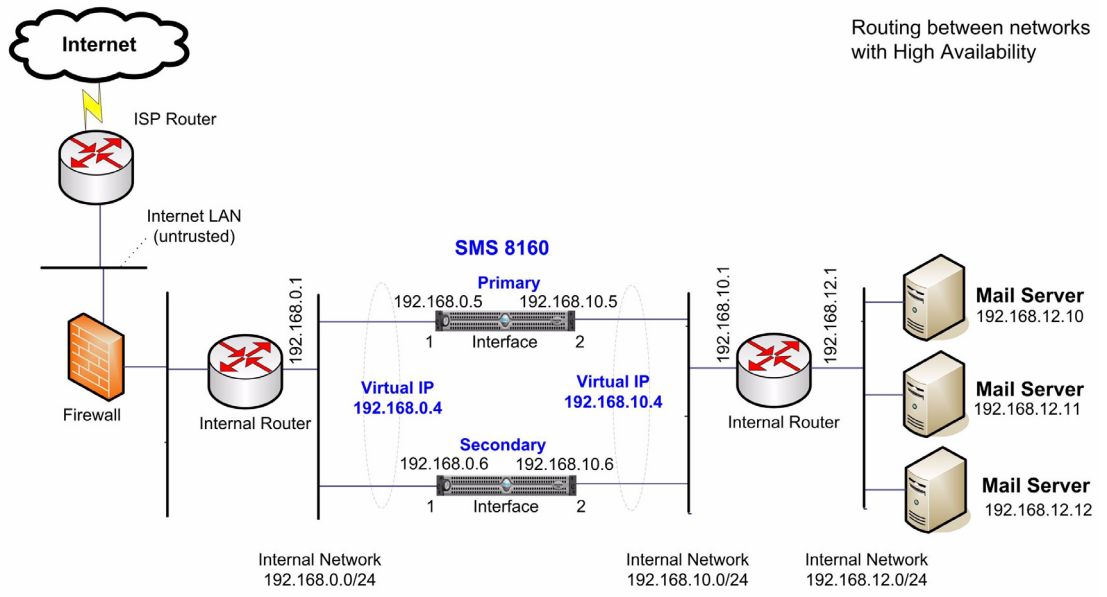


Figure A-1 Diagram of high availability virtual bridge mode configuration

High availability router implementation

The diagram below shows an installation of two Symantec Mail Security 8160 appliances in router mode, configured for high availability. In this configuration, the appliance designated as the primary appliance provides data synchronization to the secondary appliance. If the primary appliance is removed from service, the traffic flows to the secondary appliance, which has up-to-date configuration and path information. The instructions in "Setting up your appliance" on page 28 explain how to deploy two Symantec Mail Security 8160 appliances in this configuration.

Figure A-2 Diagram of high availability router mode implementation



In this example, mail from the "external network" is sent to 192.168.0.4.

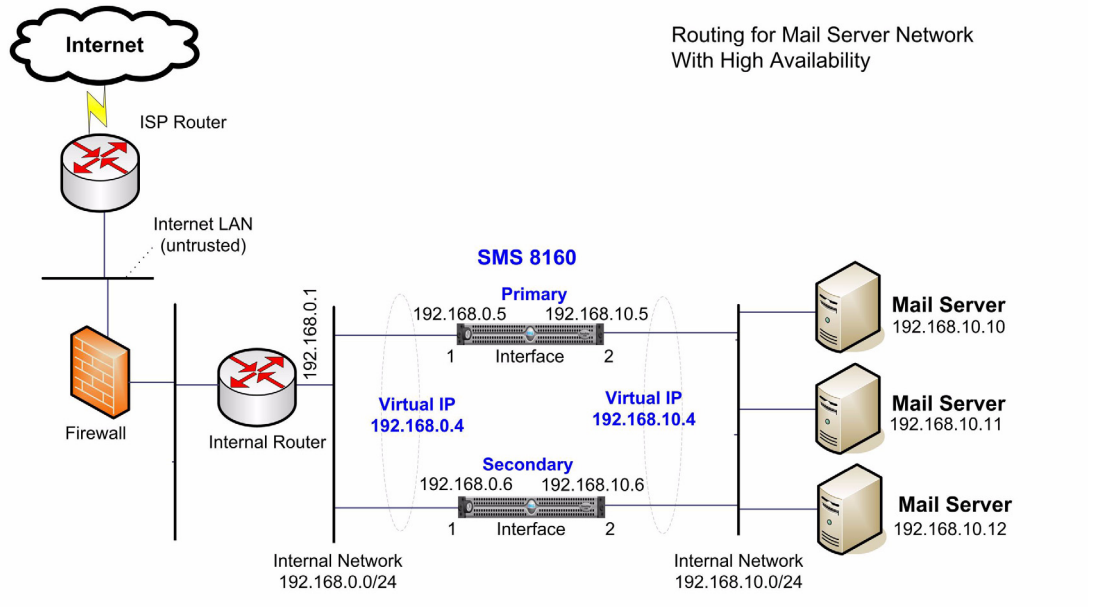
The next-hop gateway for the protected servers is 192.168.10.1.

The gateway for outbound traffic is 192.168.10.4.

Mail server gateway router implementation

In this implementation, your network is physically configured such that the only machines behind Symantec Mail Security 8160 appliances are SMTP servers. You can decrease traffic load on Symantec Mail Security 8160 by configuring your network this way.

Figure A-3 Diagram of high availability gateway router mode implementation



In this example, mail from the “external network” is sent to 192.168.0.4.

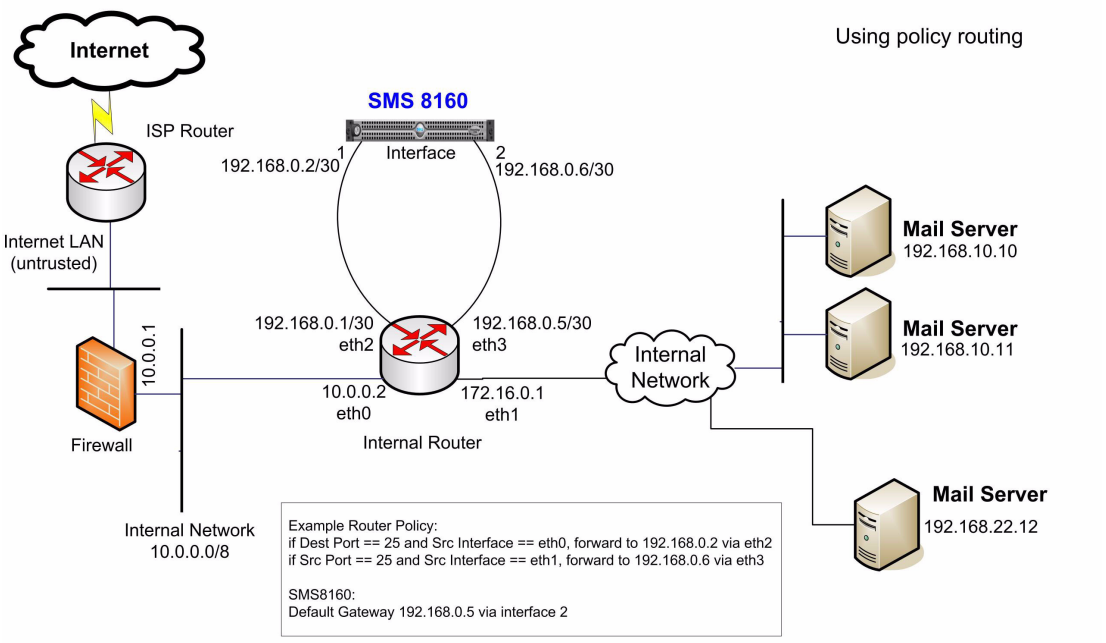
The next-hop gateway for the protected servers is 0.0.0.0.

The gateway for outbound traffic is 192.168.10.4.

Policy routed router implementation

In this implementation, only SMTP traffic flows through Symantec Mail Security 8160. You accomplish this configuring your router to policy route only SMTP traffic through Symantec Mail Security 8160. Return traffic must also be routed through the appliance. If your network carries a large amount of non-SMTP traffic and you cannot place the 8160s directly in front of the mail servers (as shown in "Mail server gateway router implementation" on page 78), you may wish to configure your Symantec Mail Security 8160 deployment this way to reduce traffic load on the appliances.

Figure A-4 Diagram of a policy routed implementation



To implement this configuration, set the default gateway on interface 2 rather than on the external interface 1 in step 16 in "To configure for high availability" on page 31.

Appendix B

Command Line Interface Reference

Each appliance has a set of commands you can use to configure, troubleshoot, and administer your system.

The following sections describe the commands available to you. To access these commands, you must open a shell session to Symantec Mail Security 8160 and log in as user **admin**. You can do this on the console, or remotely using ssh to port 22.

Caution: If you have more than one Symantec Mail Security 8160 deployed in a high availability configuration, make sure that any changes you make (for instance, using the `restore-config` command) take into account the configuration on other 8160s in your deployment.

---

bootstrap

The `bootstrap` command is run during the initial boot to configure the basic information on the appliance.

The bootstrap command has one optional switch, `--reconfigure`. Running `bootstrap --reconfigure` will erase the current configuration and allow you to start completely from scratch.

After running `bootstrap –reconfigure`, you must reinstall your license, and go through the Setup Wizard again.

After a configuration is activated, the bootstrap command exits immediately.

clear

The `clear` command clears all log files. You can use the clear command to free up disk space if you have received an alert message indicating that the appliance disk has reached 90% capacity.

grep

The `grep` command searches within the system logfiles.

help

The `help` command displays a list of available commands on the appliance.

The `help` command has the following syntax:

```
help
```

ifconfig

The ifconfig command configures the network for an appliance. This command is part of the standard Linux command set. For additional details, try typing `ifconfig -?` or refer to a Linux user's manual of your choice. Note that changes to any network interfaces made with the `ifconfig` command will be lost the next time the system boots. For permanent changes, use the Site Setup Wizard in the Control Center.

iostat

The `iostat` command is used for monitoring system input/output device loading by observing the time the devices are active in relation to their average transfer rates.

The `iostat` command has the following syntax:

```
iostat <flags>
```

netstat

The `netstat` command is used to print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. This command is part of the standard Linux command set. For additional details, try typing `netstat --help` or refer to a Linux user's manual of your choice.

The `netstat` command has the following syntax:

```
netstat <flags>
```

nslookup

The `nslookup` command performs a DNS lookup of the given hostname or IP address. This command is part of the standard Linux command set. For additional details, try typing `nslookup --help` or refer to a Linux user's manual of your choice.

The `nslookup command has the following syntax:`

```
nslookup <hostname|ip address>
```

passwd

The `passwd` command changes the password for the command line interface and Control Center login.

The `passwd` command has the following syntax:

```
passwd
```

ping

The `ping` command tests the transfer of data between the issuing machine and the given hostname or IP address. All arguments are permitted. This command is part of the standard Linux command set. For additional details, try typing ping --help or refer to a Linux user's manual of your choice.

The `ping` command has the following syntax:

```
ping <hostname|ip address>
```

reboot

The `reboot` command reboots the appliance and is part of the operating system.

The `reboot` command has the following syntax:

```
reboot
```

rebuildrpmdb

The `rebuildrpmdb` command recreates the RPM database for the appliance.

The `rebuildrpmdb` command has the following syntax:

```
rebuildrpmdb
```

restore-config

The `restore-config` command reverts from the current version to the last saved version. It takes no arguments.

route

The `route` command allows for the viewing and manipulation of the IP routing table. Its primary use is to set up static routes to specific hosts or networks via interface, after it has been configured with the `ifconfig` command.

service

The `service` command allows for the changing of status for components within the Symantec 8160 appliance.

The `service` command has the following syntax:

```
service <component_name> <command>
```

where:

- component_name can be any one of the following:
  - asrctl - the Symantec Mail Security 8160 software
  - asrconfig - the Symantec Mail Security 8160 configuration
  - osconfig - OS-level configuration
  - stunnel - the secure (SSL) connection
- command can be any one of the following:
  - start
  - stop
  - restart

showarp

The `showarp` command displays the ARP table on the appliance.

The `showarp` command has the following syntax:

```
showarp
```

shutdown

The `shutdown` command shuts down the appliance.

The `shutdown` command has the following syntax:

```
shutdown
```

system-stats

The `system-stats` command is Used to display system statistics.

The `system-stats` command has the following syntax:

```
system-stats <key>
```

where `key` can be blank, in which case all available values are returned, or one or more of the following:

- cpu_usage—Displays the CPU usage as a percentage
- disk_used—Displays the disk used in KB
- disk_free—Displays the disk free in KB
- mem_used—Displays the memory used in KB
- mem_free—Displays the memory free in KB
- swap_used—Displays the amount of swap in use
- swap_free—Displays the amount of free swap
- eth0_in—Displays the current incoming data rate in KB
- eth0_out—Displays the current outgoing data rate in KB
- eth1_in—Displays the current incoming data rate in KB
- eth1_out—Displays the current outgoing data rate in KB
- disk_in—Displays the current rate of disk writes in KB
- disk_out—Displays the current rate of disk reads in KB

tail

The `tail` command shows the last 50 lines of the `/data/logs/messages` log file. It takes no arguments.

traceroute

The `traceroute` command traces the network route to the given hostname or IP address and is part of the operating system. All arguments are permitted. This command is part of the standard Linux command set. For additional details, try typing `traceroute --help` or refer to a Linux user's manual of your choice.

The `traceroute` command has the following syntax:

```
traceroute <hostname|ip address>
```

```
update
```

```
The update command can check for new packages, download new
packages, install new packages on the appliance, and list available
versions for installation.
```

```
The update command has the following syntax:
```

update <option>

where option can be any of the following:

- check—compares installed and available packages to check whether or not your installation is current.
- download—Fetches any new packages for future installation.
- install—Installs the most recent packages to your appliance.
- list—displays a list of installations available on your appliance.

version

The `version` command displays the version of software being run by the appliance.

The `version` command has the following syntax:

```
version
```

watch

The `watch` command executes `tail -f /data/logs/messages`, sending output to the screen for monitoring.

Appendix C

SNMP MIB Reference

```
SYMANTEC-SMTP-TRAFFIC-SHAPING DEFINITIONS ::= BEGIN

IMPORTS
  NOTIFICATION-GROUP
    FROM SNMPv2-CONF
  MODULE-IDENTITY,
  OBJECT-TYPE,
  NOTIFICATION-TYPE,
  Counter32,
  Gauge32,
  Counter64,
  Unsigned32,
  enterprises
    FROM SNMPv2-SMI
  DisplayString
    FROM SNMPv2-TC;

symantecOBJECT IDENTIFIER ::= { enterprises 393 }
productsOBJECT IDENTIFIER ::= { symantec 200 }
sms OBJECT IDENTIFIER ::= { products 130 }

symantecSMTPTrafficShaping MODULE-IDENTITY
  LAST-UPDATED"200505261709Z"
  ORGANIZATION"Symantec Corporation"
  CONTACT-INFO
    "   Symantec Corporation
        20300 Stevens Creek Blvd.
```

```
        Cupertino, CA 95014
        US

        408-517-8000"
  DESCRIPTION
    "The MIB module to describe statistics and traps that apply
    to the Symantec SMTP Traffic Shaping capabilities."
  REVISION"200505261709Z"
  DESCRIPTION
    "Initial revision."
  ::= { sms 1 }

sstsPathCount OBJECT-TYPE
  SYNTAXGauge32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of known paths in the SMTP Path database."
  ::= { symantecSMTPTrafficShaping 1 }

sstsBlocklistRejected OBJECT-TYPE
  SYNTAXCounter64
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of times that connections were rejected due to
    the source path being listed as blocked."
  ::= { symantecSMTPTrafficShaping 2 }

sstsStageName OBJECT-TYPE
  SYNTAXDisplayString (SIZE (0..255))
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The name of the current stage of SMTP resource management."
  ::= { symantecSMTPTrafficShaping 3 }
```

```
sstsClassNumber OBJECT-TYPE
  SYNTAXUnsigned32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of SMTP classes present on this system."
  ::= { symantecSMTPTrafficShaping 4 }

sstsStatsTable OBJECT-TYPE
  SYNTAXSEQUENCE OF SstsClassStats
  MAX-ACCESSnot-accessible
  STATUScurrent
  DESCRIPTION
    "A list of SMTP class entries. The number of entries is given
    by the value of sstsClassNumber."
  ::= { symantecSMTPTrafficShaping 5 }

sstsClassStats OBJECT-TYPE
  SYNTAXSstsClassStats
  MAX-ACCESSnot-accessible
  STATUScurrent
  DESCRIPTION
    "An entry describing the accrued statistics pertaining to a
    given SMTP class."
  INDEX{ sstsClassStatsIndex }
  ::= { sstsStatsTable 1 }

SstsClassStats ::=
  SEQUENCE {
    sstsClassStatsIndexInteger32,
    sstsClassStatsNameDisplayString,
    sstsClassStatsConnectionLoadGauge32,
    sstsClassStatsConnectionAttemptsCounter64,
    sstsClassStatsConnectionAcceptedCounter64,
    sstsClassStatsMessagesCounter64,
    sstsClassStatsRecipientsCounter64
  }
```

```
sstsClassStatsIndex OBJECT-TYPE
  SYNTAXInteger32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The index for this row of the table."
  ::= { sstsClassStats 1 }

sstsClassStatsName OBJECT-TYPE
  SYNTAXDisplayString (SIZE (0..255))
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The name of this SMTP class, indicating the spam percentage
    that a path must have for its connections to be members of
    this class."
  ::= { sstsClassStats 2 }

sstsClassStatsConnectionLoad OBJECT-TYPE
  SYNTAXGauge32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of active connections currently attributed to this
    SMTP class."
  ::= { sstsClassStats 3 }

sstsClassStatsConnectionAttempts OBJECT-TYPE
  SYNTAXCounter64
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of connection attempts that have been made for this
    SMTP class."
  ::= { sstsClassStats 4 }
```

```
sstsClassStatsConnectionAccepted OBJECT-TYPE
  SYNTAXCounter64
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of connection attempts that have been accepted into
    this SMTP class."
  ::= { sstsClassStats 5 }

sstsClassStatsMessages OBJECT-TYPE
  SYNTAXCounter64
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of messages that have been sent by connections
    in this SMTP class."
  ::= { sstsClassStats 6 }

sstsClassStatsRecipients OBJECT-TYPE
  SYNTAXCounter64
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of message recipients that have been seen in
    messages in this SMTP class."
  ::= { sstsClassStats 7 }

sstsConfigTable OBJECT-TYPE
  SYNTAXSEQUENCE OF SstsClassConfig
  MAX-ACCESSnot-accessible
  STATUScurrent
  DESCRIPTION
    "A list of SMTP class entries. The number of entries is given
    by the value of sstsClassNumber."
  ::= { symantecSMTPTrafficShaping 6 }

sstsClassConfig OBJECT-TYPE
```

```
  SYNTAXSstsClassConfig
  MAX-ACCESSnot-accessible
  STATUScurrent
  DESCRIPTION
    "An entry describing the configuration pertaining to a given
    SMTP class."
  INDEX{ sstsClassConfigIndex }
  ::= { sstsConfigTable 1 }

SstsClassConfig ::=
  SEQUENCE {
    sstsClassConfigIndexInteger32,
    sstsClassConfigNameDisplayString,
    sstsClassConfigBandwidthUnsigned32,
    sstsClassConfigConnectionLimitUnsigned32,
    sstsClassConfigSpamLimitUnsigned32,
    sstsClassConfigConnectionsPerPathLimitUnsigned32,
    sstsClassConfigMessagesPerConnectionLimitUnsigned32,
    sstsClassConfigReconnectTimeoutUnsigned32
  }

sstsClassConfigIndex OBJECT-TYPE
  SYNTAXInteger32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The index of this row in the table."
  ::= { sstsClassConfig 1 }

sstsClassConfigName OBJECT-TYPE
  SYNTAXDisplayString (SIZE (0..255))
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The name of this SMTP class, indicating the spam percentage
    that a path must have for its connections to be members of
    this class."
```

```
  ::= { sstsClassConfig 2 }

sstsClassConfigBandwidth OBJECT-TYPE
  SYNTAXUnsigned32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The amount of bandwidth allotted to all connections in this
    SMTP class. Each connection will receive a fraction of the
    bandwidth proportional to the total bandwidth divided by the
    limit of connections in this class."
  ::= { sstsClassConfig 3 }

sstsClassConfigConnectionLimit OBJECT-TYPE
  SYNTAXUnsigned32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The total number of connections that will be allowed to
    simultaneously exist from paths that fall in this class.
    Connection attempts happening after this limit is reached
    will fall into worse SMTP classes or be rejected if those
    are also full."
  ::= { sstsClassConfig 4 }

sstsClassConfigSpamLimit OBJECT-TYPE
  SYNTAXUnsigned32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The limit on the percentage of spam sent that a path could
    have recorded in the database such that it would still be
    classified in this SMTP class."
  ::= { sstsClassConfig 5 }

sstsClassConfigConnectionsPerPathLimit OBJECT-TYPE
  SYNTAXUnsigned32
```

```
    MAX-ACCESSread-only
    STATUScurrent
    DESCRIPTION
      "The limit on the number of concurrent connections that a
      single path could have open."
    ::= { sstsClassConfig 6 }

  sstsClassConfigMessagesPerConnectionLimit OBJECT-TYPE
    SYNTAXUnsigned32
    MAX-ACCESSread-only
    STATUScurrent
    DESCRIPTION
      "The limit on the number of messages that a path could send
      during the course of a single connection."
    ::= { sstsClassConfig 7 }

  sstsClassConfigReconnectTimeout OBJECT-TYPE
    SYNTAXUnsigned32
    MAX-ACCESSread-only
    STATUScurrent
    DESCRIPTION
      "The number of seconds that a path would have to wait before
      it could reconnect after meeting its ConnectionsPerPathLimit.
      Connection attempts before this timeout expires will be
      rejected. This timeout is applied from the beginning of the
      connection."
    ::= { sstsClassConfig 8 }

  sstsDatabaseFull NOTIFICATION-TYPE
    OBJECTS{ sstsPathCount }
    STATUScurrent
    DESCRIPTION
      "This trap indicates that the SNMP agent has detected that
      the SMTP Path Database is filled to capacity and can no
      longer sustain additional insertions."
    ::= { symantecSMTPTrafficShaping 7 }
```

```
sstsDatabaseNotFull NOTIFICATION-TYPE
  OBJECTS{ sstsPathCount }
  STATUScurrent
  DESCRIPTION
    "This trap indicates that the SNMP agent has detected that
    the SMTP Path Database is no longer filled to capacity and
    can now sustain insertions. This will be fired when the
    Database becomes not full after it had previously been full."
  ::= { symantecSMTPTrafficShaping 8 }

sstsDatabaseFullNotFullNotificationGroup NOTIFICATION-GROUP
  NOTIFICATIONS{ sstsDatabaseFull, sstsDatabaseNotFull }
  STATUScurrent
  DESCRIPTION
    "The notifications which indicate specific changes in
    sstsPathCount."
  ::= { symantecSMTPTrafficShaping 9 }

END
```

Index

A

About configuration 25
About Symantec Mail Security 8160 9
Access
    Control Center 11
Access control
    SNMP 30
Access list 30
Active state 43
Addressing considerations 21
Administration 69
    paths 61
Advanced failover 19, 31, 38
    example 38
Appliance setup 28
ARP table 53

B

Back up paths data 65
Bandwidth 46
Bandwidth estimates 46
Bandwidth utilization graph 51
Blacklist
    upload 64
bootstrap command 81
Bootstrap procedure 25
Bridged
    bridged vs. routed 30
Bridged mode 16
Bridges
    high availability and virtual bridge implementation 76

C

CDROM drives 10
Changelog 69
clear command 82
CLI reference 81
    bootstrap 81
    clear 82
    grep 82
    help 82
    ifconfig 82
    install 82
    iostat 82
    nslookup 83
    passwd 83
    ping 83
    reboot 83
    rebuildrpmdb 83
    restore-config 83
    route 84
    service 84
    showarp 84
    shutdown 84
    system-stats 84
    tail 85
    traceroute 85
    update 86
    version 86
    watch 86
Clusters 18
Command Line reference 81
Configuration
    about 36
    exporting 36
    importing 36
    reverting 37
Configure
    about configuration 25
Connection limit 46
Connection load graph 51
Connection timeout 47
Connections per IP 47
Control Center 11
    access 11
    access control 30
    permissions 12
Current path statistics 50

D

Data synchronization 37
Database
    back up 65
    paths 64
Default login 26
Deployment planning 13
DNS setup 29

E

Email traffic estimates 55
Email volume
    overall performance 55
Ethernet interfaces 25
    setup 29
Event Log 54
Export
    graph data 52
External network 53

F

Failover 19, 31
    example 38
Firewall considerations 20
Front panel indicators 10

G

Graphs 50
    bandwidth utilization 51
    connection load 51
    email estimates 55
    export data 52
    message load 51
    overall performance 55
    path quality statistics 51
    time frame 52
grep command 82
Groups
    administration 69

H

help command 82
High availability 18
    addressing considerations 21
    advanced failover 38
    Bridged active-passive 19
    failover 19
    mail server gateway router implementation 78
    MX active-active 19
    Routed active-passive 19
    router implementation 77
    setup 31
    virtual bridge implementation 76

I

ifconfig command 82
Inactive state 43
Initialization procedure 25
install command 82
Interface setup
    Setup
        ethernet interfaces 29
Interfaces 29
Interfaces 1 and 2 25
iostat command 82

L

Licenses 74
Licensing 26

M

Mail server gateway router implementation 78
Manage licenses 74
Management access setup 30
Manually altered paths 63
Message load graph 51
Messages per connection 47
Multiple appliances 35
Multiple locations 20

N

netstat command
    CLI reference
        netstat 82
Network adapters 25
Network path information 59
    administration 61
    back up paths data 65
    bulk changes 63
    manually altered paths 63
    modifying 61
    path confidence 61
    paths database 64

restoring paths data 65
search 60
spam rate 61, 62
whitelist and blacklist 64
Network route setup
Setup
network routes 32
Network statistics 53
ARP table 53
external network 53
protected network 53
nslookup command 83

O

Operating modes and configuration considerations 13
Overall performance 55
email volume 55
Overflow bucket 47

P

Passthrough state 43
passwd command 83
Password
changing user passwords 70
Path statistics 50, 54
Paths
administration 61
back up data 65
bulk changes to network paths 63
confidence 61
database 64
information 59
manually altered 63
modifying 61
quality statistics graph 51
spam rate 62
whitelist and blacklist 64
Permissions 12
ping command 83
Placement considerations 20
Planning 13
addressing for high availability 21
firewall considerations 20
multiple locations 20
placement considerations 20
port access requirements 21
security considerations 22
Policy routed router implementation 79
Port access requirements 21
Power down appliance 69
Protected network 53
Protected SMTP servers 32

R

reboot command 83
rebuildrpmdb command 83
Registration 26
restore-config command 83
Restoring paths data 65
route command 84
Routed
bridged vs. routed 30
Router Mode 17
Routers
high availability and router implementation 77

S

Search
network path information 60
Security considerations 22
service command 84
Set up
alerts 73
Settings
revert 37
Setup 28
access control 30
DNS 29
high availability 31
multiple appliances 35
protected SMTP servers 32
time 29
virtual bridge vs. routed 30
showarp command 84
shutdown command 84
SNMP
access control 30
Software updates from Symantec 72
Spam rate 61
paths 62
Specifications 9
Starting services 68
Starting, stopping, or powering down 68
Statistics

path quality statistics graph 51
Stopping services 68
Supported USB CD drives 10
Synchronization 37
System Specifications 9
system-stats command 84

T

tail command 85
Threshold 45
Time
graph timeframe 52
Time settings 29
traceroute command 85
Traffic Control
about 43
active state 43
bandwidth 46
bandwidth estimates 46
change levels 44
configuration file 45
connection limit 46
connection timeout 47
connections per IP 47
inactive state 43
messages per connection 47
overflow bucket 47
passthrough state 43
threshold 45
Turn off appliance 69

U

update command 86
Updates to software 72
USB CDROM drives 10
User passwords 70
User permissions 12
Users
add new user account 70
administration 69
delete accounts 71
modify user account 72

V

version command 86
View
current path statistics 50
Virtual Bridge mode 16
Virtual bridge vs. routed setup 30

W

watch command 86
Whitelist
upload 64